Datatilsynet

Chair of the board on behalf of the board
TELENOR ASA
P.O. Box 800
NO-1331 FORNEBU

Click

Your reference	Our reference	Date
[WSWR-LEGAL.FID1258636]	21/03823-45	10.03.2025

Decision – Data Protection Officer role in Telenor ASA

1 Introduction and summary

The Norwegian Data Protection Authority (hereinafter referred to as 'Datatilsynet', 'we', 'our', 'us', 'the supervisory authority') is the competent supervisory authority pursuant to Section 20 first paragraph of the Act relating to the processing of personal data (Personal Data Act) and pursuant to Article 51 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, hereinafter 'GDPR').

We hereby adopt a decision to issue a compliance order, impose a reprimand on and an administrative fine to Telenor ASA[1] (hereinafter also referred to as 'controller', 'processor', 'company', 'enterprise', 'undertaking', 'party', 'employer', 'you' and 'your') for the reasons outlined below. Telenor ASA is separate from the Telenor Group (hereinafter also referred to as the 'Group'), which consists of the parent company and subsidiaries (hereinafter also referred to as 'business units').

Other concerned supervisory authorities in the EEA countries where Telenor has business units (Denmark, Sweden and Finland) were consulted before the decision was adopted.

Excerpts from documents not available in Norwegian have been reproduced in the original language. This includes Telenor ASA's internal documents and job titles. For documents from EU bodies, the Danish language version, alternatively English, is used.

Summary
After having received anonymous tips, Datatilsynet launched an inspection into Telenor ASA's compliance with the data protection officer ('DPO') requirements set out in Articles 37–39 GDPR and the organisational requirements set out in Article 24 GDPR. Based on the inspection, our conclusion is that Telenor ASA has violated Articles 37(7), 38(2), 38(3), 24(1) and 24(2) GDPR during the timeframe of the inspection. As a result of the inspection, we issue a compliance order, impose a reprimand on and an administrative fine to Telenor ASA, as further described in section 2.

2 Decision

Pursuant to Article 58(2)(d) GDPR and Article 24(1) and (2) GDPR, we hereby impose the following orders on Telenor ASA:

- *To carry out a documented internal assessment of whether Telenor ASA is obliged to appoint a data protection officer (DPO), which, among other things, takes into account Telenor ASA's role in the various processing activities.*

[1] Telenor ASA is the parent company of the Telenor Group.

- *To revise the record of processing activities, cf. Article 30 GDPR, and implement organisational measures to ensure that it at all times reflects an updated description of Telenor ASA's processing activities, the number of data subjects and Telenor ASA's roles.*

- *In the event that Telenor ASA is actually obliged to have a DPO, to implement organisational measures and appropriate policies with regard to the DPO's organisation. This includes a description of the reporting line to a clearly defined highest management level, a description of the tasks the DPO should be involved in, as well as the manner and timing of such involvement. Assessments and measures to ensure independence and to avoid conflicts of interest include clearly distinguishing between any other roles in the job description, providing a separate email address for the DPO and carrying out a documented assessment of the DPO's shareholding in the company.*

Pursuant to Article 58(2)(b) GDPR, cf. Article 38(3) last sentence, we hereby impose a reprimand on Telenor ASA for:

- *not having a direct reporting line in place for the DPO of Telenor ASA to the highest management level for approximately one year of the timeframe of the inspection.*

Pursuant to Article 58(2)(i) GDPR and Section 26 of the Norwegian Personal Data Act, we hereby impose an administrative fine against Telenor ASA in the amount of ***NOK 4,000,000*** *for:*

- *not having implemented appropriate organisational measures to ensure and demonstrate compliance with the GDPR, in violation of Article 24(1) GDPR, and for not having implemented appropriate data protection policies, in violation of Article 24(2) GDPR.*

3 Background to the case

In 2021, the management of Datatilsynet decided to carry out an on-site inspection of Telenor ASA. The object of the inspection was to clarify Telenor ASA's compliance with the data protection officer requirements set out in Articles 37–39 GDPR and the requirements for appropriate organisational measures set out in Article 24 GDPR.

The original plan was to carry out the on-site inspection on 7 January 2022. However, due to the Norwegian Government's restrictions in relation to the Covid-19 pandemic, the inspection had to be postponed to 28 January 2022, at which time Datatilsynet held several interviews with executives and employees of Telenor ASA via video conference calls. The inspection and interviews concerned factual circumstances in the period from 10 October 2020[2] until the

[2] The date when Datatilsynet was first notified of then DPO [redacted]. See the final inspection report of 30 September 2022, p. 2.

interviews were conducted on 28 January 2022 (hereinafter referred to as the 'timeframe of the inspection').

In our inspection notice dated 26 November 2021, we asked Telenor ASA for specific documentation, which we received on 13 December 2021. We also asked for additional documentation on 22 December 2021, which we received on 9 January 2022. Moreover, after the interviews on 28 January 2022, we asked Telenor ASA to disclose their record of processing activities, which we received on 2 February 2022. We sent our preliminary inspection report to Telenor ASA on 11 April 2022 and received their comments on 16 May 2022. Telenor ASA's comments have been addressed and incorporated into the final inspection report.

For further details regarding the factual background to the present case, we refer to our final inspection rapport dated 30 September 2022.

The new Director General of Datatilsynet, Line Coll, was appointed on 1 August 2022. In summer 2023, Coll concluded that she was disqualified from considering the case due to impartiality following her former role as partner in the law firm Wikborg Rein, where she had provided legal counselling to Telenor ASA regarding Datatilsynet's inspection. A request was sent to the Ministry of Local Government and Regional Development to appoint an acting director general for the case. The Ministry concluded on 20 November 2023 that Coll was disqualified from considering the case. Pursuant to Section 6 third paragraph of the Norwegian Public Administration Act, a case in which the superior official is disqualified may not be decided by any directly subordinate official in the same administrative agency. However, according to theory and the interpretation of the wording of Section 6 third paragraph, Datatilsynet's employees may assist in handling the case and preparing decisions.

The Ministry appointed Mona Naomi Lintvedt as Acting Director General for this case, and the decisions in the case were made under her direction. Since the final inspection report was finalised after Coll took office, the Acting Director General has considered whether the disqualification would affect the validity of the report. In an assessment dated 30 December 2023, she concluded that the final report did not contain any assessments or decisions, but only described the facts and findings of the inspection, and that it was therefore not affected by the disqualification of Datatilsynet's Director General and employees.

An advance notification was issued on 1 March 2024 pursuant to Section 16 of the Public Administration Act[3] to enable the company to make written representations in relation to the case before a decision was made.

Datatilsynet considers this to be a cross-border case in which the cooperation mechanism in Article 60 GDPR applies, which means that a draft decision will be shared with the competent supervisory authorities in the EEA.[4] See also section 4.1 below. Due to the aforementioned European cooperation and the fact that Telenor ASA's working language is English, the

[3] Act of 10 February 1976 relating to procedure in cases concerning the public administration (Public Administration Act).
[4] European Economic Area

advance notification was originally written in English. At the request of Telenor ASA's lawyer, we prepared a Norwegian version of the notification, which was sent to the company on 18 April 2024. In the event of conflict, the Norwegian text shall take precedence. Wikborg Rein, on behalf of Telenor ASA, submitted their comments on the advance notification on 31 May 2024 (hereinafter also referred to as the 'response').

4 Legal background

4.1 Competence, tasks and powers of supervisory authorities under the GDPR

We refer to Articles 55(1), 56(1) and 58(2) GDPR regarding Datatilsynet's competence, tasks and powers. We further refer to Article 83(1) to (5) GDPR regarding the imposition of administrative fines and to Section 26 first paragraph of the Personal Data Act.

Article 3(1) GDPR reads as follows:

> 'This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.'

The Telenor Group has operations and business units/offices ('BUs') both in and outside the EEA:

> 'The Telenor Group (of companies) consists of several autonomous legal entities, registered both in Norway and across the globe, with separate Boards of Directors. This includes the administrative headquarters and Group parent company Telenor ASA, and various "Business Units" (BUs), which are subsidiaries directly or indirectly controlled by Telenor ASA'.[5]

Pursuant to Article 3(1) GDPR, the GDPR applies to all processing of personal data by Telenor ASA where the company acts as controller, joint controller and/or data processor, regardless of whether the processing activities take place in or outside the EEA.

With respect to the processing activities covered by the scope of the inspection, Telenor ASA qualifies as controller (cf. Article 4(7) GDPR) or processor (cf. Article 4(8) GDPR), depending on the processing at hand.[6] As controller and processor, Telenor ASA has its main establishment in Norway, cf. Article 4(16) GDPR.

We consider the processing activities that fall within the scope of the present case to qualify as 'cross-border processing' under Article 4(23) GDPR. In its comments on the advance notification, Telenor ASA claims that the case is not of a cross-border nature because it does not concern specific processing activities and – alternatively – because the processing does

[5] 'Response to Datatilsynet', 13 December 2021, p. 1.
[6] 'Response to Datatilsynet', 13 December 2021, p. 1.

not meet the requirement of Article 4(23)(b) GDPR, in particular the condition that concerns data subjects in more than one member state being 'substantially' affected.[7]

We have considered Telenor ASA's arguments, but uphold our assessment, which we will elaborate on in more detail below.

First and foremost, it should be emphasised that, since the DPO must be involved in 'all' issues that relate to the protection of personal data, cf. Article 38(1) GDPR, the present case covers *all* processing of personal data that takes place in connection with activities in Telenor ASA. The documentation that Telenor ASA has sent to Datatilsynet shows that a wide range of processing activities take place in connection with activities in Norway and in other countries, both in and outside the EEA. The record of processing activities refers to several 'countries of processing' in the EEA (Denmark, Sweden, Finland etc.)..[8] Several of these processing activities actually concern the personal data of employees throughout the Telenor Group, which means that they take place in connection with activities in several Telenor business units in and outside the EEA. This in itself meets the requirement set out in Article 4(23)(a).

We note that, in the sense of the GDPR, 'establishment' entails 'the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect'.[9] In other words, the term 'establishment' does not only cover the place where the controller or processor is formally incorporated; it also covers subsidiaries, branches and agents abroad, such as 'all Telenor companies' in the EEA, cf. the column 'recipients of personal data' in the record of processing activities. Therefore, we believe it is not correct, as claimed in the response, that '[g]iven that Telenor ASA is only established in Norway, only the provision in (b) can form the basis for characterising the processing as cross-border processing'.[10] Telenor ASA has, in the sense of the GDPR, several establishments in the EEA, and it is therefore not only the provision in (b) that can form the basis for characterising the processing.

In addition, in order to determine that the processing takes place 'in the context of the activities of establishments' of a controller or processor, it does not need to be carried out directly by that establishment.[11] It is enough that the processing is related to the activities of that company. Accordingly, the condition set out in Article 4(23)(a) GDPR is met with respect to the processing activities described in the record of processing activities with several EEA countries ('countries of processing') or involving Telenor subsidiaries or branches in the

[7] Comments on the advance notification of 31 May 2024, pp. 21–24.
[8] Telenor ASA's Article 30 record of 2 February 2022.
[9] GDPR Recital 22, and European Court of Justice case C-191/15, *Verein für Konsumenteninformation*, paragraphs 75–76.
[10] Comments on the advance notification of 31 May 2024, p. 22.
[11] CJEU case C-131/12, *Google Spain*, paragraphs 52–53, and CJEU case C-230/14, *Weltimmo*, paragraphs 25 and 35.

EEA, such as with respect to employees throughout the Telenor Group (and not only employees of Telenor ASA).[12]

Moreover, there are processing activities that take place in connection with the establishment in Norway, but which substantially affect or are likely to substantially affect data subjects in more than one EEA country. This is the case, for example, with regard to 'multi-year surveys in Telenor's markets to understand customer behaviours', which, according to the record of processing activities, affect [redacted] customers in several EEA countries through an analysis of their behaviour that may be particularly intrusive. The same applies when processing activities in Norway affect all employees in the Telenor Group, such as 'Learning Management Systems' and 'Employee Share Plan', which, according to the record of processing activities, affect [redacted] data subjects. In our final inspection report, we find that the number of employees in the Telenor Group during the timeframe of the inspection is approximately 15,000.[13] In this regard, it must be noted that the consistency mechanism for cooperation between supervisory authorities applies when processing activities substantially affect a *significant number of* data subjects in several EEA countries, cf. GDPR Recital 135. We find that the condition concerning a significant number is met. We emphasise that the condition concerning data subject being substantially affected is not a requirement under Article 4(23)(a) GDPR, but only under (b), and it is therefore not strictly necessary to demonstrate that the requirement is met in this case. In any case, the threshold is low for what is considered to significantly affect data subjects. The EDPB's guidelines assume, for example, that it is sufficient if the actual processing in question affects or is likely to affect individuals' 'health, well-being and peace of mind.'[14]

The documentation collected by Datatilsynet has shown that Telenor ASA has internal procedures and policies[15] that are the same in all countries in which the Telenor Group operates, thus affecting data subjects in several EEA countries. We assume that Telenor ASA as the parent company and controller has the power to change and influence group policies.[16] The inspection has revealed that Telenor ASA, in addition to being the controller for certain data processing activities, sometimes acts as processor on behalf of other business units and may also act as joint controller with other business units, which in itself entails a cross-border element.[17]

---

[12] In this regard, it should be noted that, when the record of processing activities refers to the processing of employees' personal data, it refers to several thousand employees. It is therefore obvious not only employees of Telenor ASA, cf. the columns 'data subject categories' and 'number of data subjects' in the record of processing activities.

[13] Final inspection report of 30 September 2022, p. 11.

[14] Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority, version 2.0, adopted 28 March 2023, p. 5-6.

[15] Group Manual Privacy

[16] 'Response to Datatilsynet', 13 December 2021 p. 1 reads as follows: 'The Telenor Group (of companies) consists of several autonomous legal entities, registered both in Norway and across the globe, with separate Boards of Directors. This includes the administrative headquarters and Group parent company Telenor ASA, and various 'Business Units' (BUs), which are subsidiaries directly or indirectly controlled by Telenor ASA.'

[17] Final inspection report of 30 September 2022, p. 6.

The cooperation mechanism and procedure laid down in Articles 56(1) and 60 GDPR therefore apply in this case. Datatilsynet is competent to act as lead supervisory authority in the case pursuant to Article 56(1). Pursuant to Article 60 GDPR, Datatilsynet shall cooperate with the other supervisory authorities concerned. This entails exchanging relevant information about the case and submitting a draft decision to the other supervisory authorities concerned so that they can issue an opinion. Due account shall be taken of their views when deciding on the case.

4.2 **EEA and Norwegian law**

The GDPR has been incorporated into Annex XI to the Agreement on the European Economic Area ('EEA Agreement') by means of Decision of the EEA Joint Committee No 154/2018 ('EEA Joint Committee Decision').[18]

Article 1(b) of the EEA Joint Committee Decision provides that:

> '[…] the terms "Member State(s)" and "supervisory authorities" shall be understood to include, in addition to their meaning in the Regulation, the EFTA States and their supervisory authorities, respectively.'

Furthermore, Article 1(c) of the EEA Joint Committee Decision reads as follows:

> 'References to Union law or Union data protection provisions shall be understood as referring to the EEA Agreement or data protection provisions contained therein, respectively.'

The Personal Data Act incorporated the GDPR into Norwegian law. The Personal Data Act and the GDPR entered into force in Norway on 20 July 2018.

5 Designation of data protection officer – Article 37

5.1 **Inspection criteria and evidence**

Article 37 GDPR reads as follows:

1) The controller and the processor shall designate a data protection officer in any case where:

    a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

[18] Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement OJ [2018] L 183/23.

b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10.

2) A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

3) Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

4) In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

5) The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

6) The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

7) The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

We further refer to sections 3.1.1 and 3.1.2 in the final inspection report of 30 September 2022.

Article 30 GDPR reads as follows:

1) Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

    a. the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
    b. the purposes of the processing;
    c. a description of the categories of data subjects and of the categories of personal data;
    d. the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

e. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
f. where possible, the envisaged time limits for erasure of the different categories of data;
g. (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

2) Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:
   a. the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
   b. the categories of processing carried out on behalf of each controller;
   c. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
   d. (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

3) The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

4) The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

5) The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

5.2 **Datatilsynet's assessment**

5.2.1 **Concerning the designation of a DPO**

Telenor ASA had designated a qualified DPO within the meaning of Article 37(5) GDPR throughout the timeframe of the inspection and had communicated the contact details to us. This is undisputed.

Whether Telenor ASA fell within Article 37(1), under which the designation of a DPO is mandatory, or whether it was a voluntary arrangement was never an issue during the inspection. This was therefore not discussed further in the inspection report or in the notification of the decision. It was assumed in the case that Telenor ASA had appointed a DPO, in which case it follows from the European Data Protection Board's (EDPB) Guidelines on Data Protection Officers that the requirements for the role set out in Articles 38 and 39 are the same as for cases where the designation of a DPO is mandatory.[19]

After receiving an advance notification, Telenor ASA stated in a letter dated 31 May 2024 that the company's DPO function had been terminated because they believed that the company's processing activities do not fall under the requirement for mandatory designation set out in Article 37. Datatilsynet was formally notified of the termination on 11 June 2024. Telenor ASA did not elaborate on why they had found that the company was not required to appoint a DPO, but assumes this as a fact without further documentation.

We reproduce the following from the EDPB's Guidelines on Data Protection Officers:

> 'When an organisation designates a DPO on a voluntary basis, the requirements under Articles 37 to 39 will apply to his or her designation, position and tasks as if the designation had been mandatory.'[20]

We find that the requirements in Articles 37–39 GDPR are applicable in this case under any circumstances. Whether Telenor ASA is obliged to have a DPO or not cannot influence the assessment of sanctions, including the amount of an administrative fine.

The above guidelines also state:

> 'Unless it is obvious that an organisation is not required to designate a DPO, the WP29 recommends that controllers and processors document the internal analysis carried out to determine whether or not a DPO is to be appointed, in order to be able to demonstrate that the relevant factors have been taken into account properly.'[21]

The EDPB refers to Article 24(1) GDPR in this context and continues:

> 'This analysis is part of the documentation under the accountability principle',[22] cf. Article 5(2) GDPR.

In our notification of the on-site inspection of 26 November 2021, we specifically requested documentation on the designation of the DPO as part of the internal control, cf. Article 24(2)

---

[19] WP 243 rev.01 'Guidelines on Data Protection Officers' adopted on 13 December 2016, last revised and adopted on 5 April 2017, approved by the EDPB in Endorsement 1/2018 of 25 May 2018, p. 5.
[20] WP 243 rev.01 'Guidelines on Data Protection Officers', p. 6
[21] WP 243 rev.01 'Guidelines on Data Protection Officers', p. 5–6
[22] WP 243 rev.01 'Guidelines on Data Protection Officers', p. 6.

GDPR.[23] A documented internal assessment of the basis on which Telenor ASA's DPO was appointed was not submitted to Datatilsynet, not then or at a later date. Such documentation is necessary to be able to demonstrate that you have carried out a genuine assessment in which all relevant factors have been taken into account. We therefore assume that such an assessment did not exist. Such an assessment should be carried out in accordance with the accountability principle unless it is obvious that the company is not obliged to designate a DPO, which is not obvious in this case. At no stage during the inspection, either in writing or orally, have you mentioned or claimed that you believe that Telenor ASA's DPO has operated on a voluntary basis. That claim only appears in your comments on the advance notification. So far, we have understood that it was agreed that Telenor ASA is obliged to have a DPO, based on the information provided by Telenor ASA during the inspection.

To be able to answer the question of whether Telenor ASA is obliged to designate a DPO pursuant to Article 37(1)(b) GDPR, it must be considered whether Telenor ASA's core activities in its role as controller or processor consist of processing operations that, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale. Telenor ASA claims that the company does not process 'personal data about employees in any other way or to a greater extent than is usual and necessary for other companies with employees. The processing is related to appointments, payroll, personnel administration, training and other routine activities that require handling of employees' personal data. These processing activities constitute necessary support functions and must be considered side activities, not core activities.'[24]

It is undisputed that necessary personnel administration and regular IT support are standard in all enterprises and are not considered core activities. For that matter, Telenor ASA has not reported what its core activities are.[25] In your comments of 31 May 2024, the company is described as follows:

> 'an administrative company with very limited operational activities, with a limited number of office employees and with mainly low-risk processing activities. Telenor ASA is not a telecom operator and nor does it provide such services to corporate or retail customers. Telenor ASA is primarily the controller for the processing of personal data about its own employees and its own suppliers etc., and otherwise has a limited role as processor in certain relations.'

We would also like to remind you that the obligation to designate a DPO is not only incumbent on the controller, but also the processor. When assessing whether the company is obliged to have a DPO, Telenor ASA must therefore take into account not only the processing

[23] Advance notification of decision of 18 April 2024, page 2: 'Datatilsynet requests that the following information/documentation be sent to us by 13 December 2021, cf. Article 58(1) GDPR:
b) Instructions/procedures for the following parts of the internal control, cf. Article 24(2) GDPR:
1) Designation of the data protection officer
2) The DPO's access to the company's management.
3) The management's involvement of the DPO in all issues relating to the protection of personal data.
4) Management review of the internal control.'
[24] Comments on the advance notification of 31 May 2024, p. 20.
[25] Comments on the advance notification of 31 May 2024, p. 12.

activities it carries out as controller, but also as processor. All processing activities[26] in the company must be considered when deciding on this issue. As explained in more detail in the following sections, the record of processing activities shows that Telenor ASA carries out far more processing activities of a greater scope than simple HR tasks. In our opinion, it is not obvious that Telenor ASA's processing activities are as limited as claimed in the response. On the contrary, the response confirms that Telenor ASA carries out processing activities that include more than just the processing of HR data for employees of Telenor ASA, and that Telenor ASA also acts as processor.[27]

As we will return to, Article 24(1) GDPR requires that the controller implements appropriate organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR, which demands internal control.[28] It is undisputed in Norwegian law theory that the assessment of an undertaking is obligated to design a DPO shall be documented and is a part of then internal control pursuant to Article 24 GDPR.[29] This is necessary to ensure and be able to demonstrate compliance like Article 24 requires. When Telenor ASA was not able to demonstrate such documented assessment, it thus is a violation of Article 24 GDPR.

5.2.2 **On the obligation to keep records of processing activities under Article 30 GDPR**

It is undisputed that Telenor ASA is obliged to keep a record of processing activities in accordance with Article 30 GDPR, and that the company does not fall under the exception in Article 30(5) as it has more than 250 employees. A record of processing activities must include a description of the purposes of processing, categories of personal data, categories of data subjects and the role of Telenor ASA as controller, joint controller and/or processor. Datatilsynet requested a copy of the record of processing activities at the end of the day of the inspection, 28 January 2022. Telenor ASA sent us the record in an email on 2 February 2022, without a disclaimer.

Telenor ASA makes a point that the record of processing activities 'was not requested by Datatilsynet until the summary meeting at the very end of the day of the inspection'[30] and that 'the record was not an issue when the inspection was carried out'.[31] Furthermore, Telenor ASA claims that the information in the record of processing activities has also not been subject to contradiction and that 'the company's attempt to explain the processing activities that take place in Telenor ASA has not been followed up by Datatilsynet'.[32]

---

[26] See Article 38(1) GDPR on the involvement of DPOs in *all* issues relating to the protection of personal data and Article 4(2), which defines 'processing'.
[27] Comments on the advance notification of 31 May 2024, pp. 14–18.
[28] Åste Marie Bergseng Skullerud, Cecilie Rønnevik, Jørgen Skorstad og Marius Engh Pellerud: *Personopplysningsloven og personvernforordningen (GDPR), kommentarutgave* (2019) p. 273
[29] Jarbekk et al: *Personopplysningsloven og personvernforordningen med kommentarer* (2019), p. 256-257.
[30] Comments on the advance notification of 31 May 2024, p. 11.
[31] Comments on the advance notification of 31 May 2024, p. 13.
[32] Comments on the advance notification of 31 May 2024, p. 13.

Datatilsynet is of the opinion that this is not correct and that Telenor ASA has been given several opportunities for contradiction in accordance with the Public Administration Act Section 17.

We emphasise the obligation in Article 30(4) GDPR that the record must be available to Datatilsynet on request. This is a key document that provides an overview of the scope of processing activities that takes place in an enterprise. This applies regardless of whether the record of processing activities is subject to inspection or, as in this case, whether other matters are being investigated. There is therefore no doubt that Telenor ASA was not only obliged to keep a record of processing activities, but that it was also obliged to make this record available to Datatilsynet on request.

We emphasise again that the obligation to keep an updated record of processing activities that meets the requirements of Article 30 is incumbent on Telenor ASA as controller and processor. We refer to section 13.2.

5.2.3 Concerning the content of the record of processing activities, including Telenor ASA's role and division of responsibilities

Datatilsynet incorporated relevant information in the record of processing activities in its preliminary inspection report of 11 April 2022. Telenor ASA provided its comments on the report in a letter of 16 May 2022. Telenor ASA's comments were incorporated into the final inspection report of 30 September 2022. In a letter of 2 November 2022, we gave you an opportunity to state your opinion on what should be exempt from public disclosure, cf. the Freedom of Information Act Section 13 first paragraph and the Public Administration Act Section 13 second paragraph (2). In connection with this, Telenor ASA submitted a second round of comments and appendices on the report in a letter dated 24 November 2022. Telenor ASA's input was taken into account in the advance notification that was sent to Telenor ASA for contradiction, first in English on 1 March 2024 and then in Norwegian on 18 April 2024. Telenor ASA submitted its comments on the notification and the inspection report with appendices in a letter dated 31 May 2024, which contained some new claims and information.

Among other things, the letter[33] stated:

> 'Telenor does not dispute that, under the circumstances, the structure of the record of processing activities may appear difficult to grasp and therefore cause some confusion. The decisive factor, however, is what type of processing activities actually take place in Telenor ASA.'

Datatilsynet considers that Telenor ASA has been given ample opportunity to clarify what they consider to be unclear, but not least, this emphasises the importance of having an accessible, reliable and clear record of processing activities in place as part of the mandatory

[33] Comments on the advance notification of 31 May 2024, p. 11.

internal control, cf. Article 24 GDPR.[34] The record forms part of the evidence investigated during the timeframe of the inspection and must contain factual descriptions of the processing activities that actually take place. Telenor ASA's claim that we 'appear to hold Telenor ASA accountable for the activities that take place in Telenor Norge AS'[35] is unfounded and not correct. The scope of the inspection is Telenor ASA and the processing activities that Telenor ASA is responsible for as controller, joint controller and/or processor.

Furthermore, after the inspection had been carried out, Telenor ASA had the opportunity to clarify and change the record to make it more up to date if necessary. It appears from the response that the company was aware that the record was not complete or appropriately structured.[36] Although this was not the subject of the inspection, Telenor ASA had and continues to have a vested interest in ensuring that the record of processing activities meets the requirements of Article 30. The record constitutes important documentation for both internal and external use and should be updated as necessary. The purpose is precisely to ensure that the record documents actual processing activities, as the company itself refers to in its response. As Telenor ASA states, the record of processing activities was created by different people filling in information:

> 'As mentioned, the entries in the record were written by employees in the line organisation who know the individual activities well, but who do not necessarily have special knowledge of the GDPR, or who otherwise maintain a level of legal precision.'[37]

If it was known that the quality was poor, it would be natural for someone to be assigned responsibility for overseeing the record as an overall document, as an obligatory organisational measure cf. Article 24(1) GDPR. Pursuant to Article 24(1) GDPR the company shall implement measures precisely to ensure and demonstrate GDPR compliance, including the duty to ensure that the record of processing activities is correct and updated at all times cf. Article 30 GDPR.[38] This is also something the DPO could have been involved in, cf. Article 38(1) GDPR. The record of processing activities also constitutes an important tool for the DPO to be able to maintain an overview of the company's processing activities, and thus also to determine which areas the DPO should become involved in.

In its response, Telenor ASA mention that the record of processing activities does not reflect its actual processing activities. This is something they have had several opportunities to comment on to Datatilsynet. We maintain that, also on this point, Telenor ASA has been given an opportunity for contradiction during the course of the case. Telenor ASA has

---

[34] Åste Marie Bergseng Skullerud, Cecilie Rønnevik, Jørgen Skorstad and Marius Engh Pellerud: *Personopplysningsloven og personvernforordningen (GDPR), kommentarutgave* (2019) p. 273, Eva Jarbekk et al.: *Personopplysningsloven og personvernforordningen med kommentarer* (2019) p. 257.
[35] Comments on the advance notification of 31 May 2024, p. 9.
[36] Comments on the advance notification of 31 May 2024, p. 13.
[37] Comments on the advance notification of 31 May 2024, p. 14.
[38] Åste Marie Bergseng Skullerud, Cecilie Rønnevik, Jørgen Skorstad & Marius Engh Pellerud: *Personopplysningsloven og personvernforordningen (GDPR), kommentarutgave* (2019) pp. 273 and 304, Eva Jarbekk et al.: *Personopplysningsloven og personvernforordningen med kommentarer* (2019) pp. 257 and 280.

submitted some new information in the response that complements the information we have received previously.

It appears from Telenor ASA's record of processing activities that Telenor ASA processes personal data about its own employees (current, former and potentially future), next of kin and family members of employees, customers of the Telenor Group, suppliers, other contractual partners, consultants, hired resources, visitors (on site and online), board members and members of the Corporate Assembly and the nomination committee.[39]

Furthermore, it is clear from the record that Telenor ASA also processes personal data provided by other subsidiaries of the Telenor Group; see also section 3.3.2 in the final inspection report.[40] First and foremost, this concerns personal data about employees of the Telenor Group (approximately 15,000[41]), but also to a limited extent about customers.[42]

In the record, Telenor ASA describes that they act as controller for many processing activities, including internal notification, investigations, surveys, audio recordings of meetings, evaluations, talent development, nonconformity reports etc. from the following entities: Group Internal Audit & Investigation, Group Legal, Group People & Sustainability and Group Strategy & Ext. Relations.[43]

In two instances, Telenor ASA states that have joint controllership. In its comments on the advance notification,[44] Telenor ASA states that 'there are or have been very few instances where the Group has joint controllership' and that they believe it 'is incorrect when the supervisory authority, for example, seems to assume that we have joint controllership to any significant degree'. Datatilsynet finds that, in this context, the number of processing activities is less important than, for example, the nature and scope of the activities, including the number of data subjects and/or purposes that require regular and systematic monitoring on a large scale, cf. Article 37(1)(b).

One processing activity concerns HR information processed in the system [redacted] by Group People & Sustainability for all employees in the Group (approx. 15,000). Telenor ASA explains:

> '[redacted] is Telenor's core HRIS maintaining an overview of all of our employees and the organizational structure. [redacted] contains employees [sic] personal information, job/role and employment related details, compensation and benefits overview, career profile details and talent related data.'[45]

In its comments on the notification, Telenor ASA mentions that they:

---

[39] Telenor ASA's Article 30 record of 2 February 2022.
[40] Final inspection report of 30 September 2022, pp. 5–10.
[41] Final inspection report of 30 September 2022, p. 11.
[42] Telenor ASA's Article 30 record of 2 February 2022; final inspection report of 30 September 2022, pp. 5–6.
[43] Telenor ASA's Article 30 record of 2 February 2022.
[44] Comments on the advance notification of 31 May 2024, p. 13.
[45] Telenor ASA's Article 30 record of 2 February 2022.

> ‘probably to a somewhat greater extent during the timeframe of the inspection than is the case today, had an IT administrator role in place who was responsible for the tools that the Telenor Group uses to handle employee information [redacted] as well as to facilitate information to and interaction between employees [redacted]. Also during the timeframe of the inspection, it was clear from a legal point of view that it was the individual company in the Telenor Group that used the system that was the controller as regards its own use.’[46]

It is the processing activities during the timeframe of the inspection that form the basis for the decision. According to the record of processing activities, Telenor ASA describes that they have joint controllership for the [redacted] processing activities. The fact that the individual company in the Telenor Group has controllership for the processing does not in any way reduce the responsibility that rests with Telenor ASA as joint controller. It is not the case that joint controllers necessarily have the same degree of responsibility.[47] Datatilsynet notes that Telenor ASA states that, during the timeframe of the inspection, they processed employee data on behalf of the whole Group, both as joint controller and as processor.[48]

The second processing activity for which Telenor ASA states that the company has joint controllership concerned [redacted], which, according to the record, was put on hold, but was scheduled to restart in the first quarter of 2022. It appears that the data subjects are customers, and the number is estimated to be [redacted]. The processing is described by Telenor ASA as follows: ‘Processing of aggregated market research data (customers and non-customers) to produce charts, overviews, summary tables – and executive level reporting.’[49]

In addition, Telenor ASA describes in the record of processing activities that they act as processor for several different processing activities. Group Internal Audit & Investigations processes internal audits that affect current and former employees, consultants, suppliers and customers, and the number of data subjects is given as [redacted].

Telenor Research under Group Strategy & Ext. Relations acts as processor for, among other things, the following: [50]

Multi-country, multi-year surveys in Telenor’s markets to understand customer behaviours.	Customers
The purpose of the processing activity is to train machine learning algorithms on audio and transcription data for speech recognition. The data comes from Telenor Norway.	Current Employees; #Customers

[46] Comments on the advance notification of 31 May 2024, p. 12.
[47] See for example CJEU cases C-210/16, *Wirtschaftsakademie,* EU:C:2018:388, paragraph 43; C-2517 *Jehova’s witnesses,* ECLI:EU:C:2018:551, paragraph 66.
[48] Comments on the advance notification of 31 May 2024, p. 12.
[49] Telenor ASA’s Article 30 record of 2 February 2022.
[50] Telenor ASA’s Article 30 record of 2 February 2022.

The categories of personal data listed are:

> 'Behavior;#Demographics;#Ownership and possessions;#Electronic devices and usage;#Communication;#Preferences or interests;#Contact details;#Family, Family;#Communication;#Electronic devices and usage;#Contact details;#Location;#Identification;#Life history and events;#Behavior;#Preferences or interests;#Location'[51]

The number of data subjects involved in processing activities for which Telenor ASA acts as processor is stated to a minimum of 100–250 to a maximum of 25K–100K.[52]

In our inspection report, we wrote the following on pp. 8–10:

> 'The former DPO of Telenor ASA has repeatedly pointed out unclarified issues with regard to controllership. In the PowerPoint presentation presented to the GU Forum on 9 September 2021, the following risks were highlighted:
>
> > 'Internal data sharing governance – Personal data is shared between business units within Telenor without adequate data sharing governance, including legal transfer mechanisms, clear definition of controller/processor relationships, and generally diffusion of responsibility.'[53]
>
> - 'Lack of transparency into existing agreement setups [+I/P]
> - Often symptoms showing of unclear division of responsibility [+I/P]
> - Lack of knowledge re. differing legal requirements in TN-regions [+I/P]
> - Differing opinions and non-standardization of roles and terms for business initiative governance [+P]'[54]

In relation to the description above, Telenor ASA has commented that it is misleading because the concerns were related to the processing that Telenor ASA mainly carries out, i.e. the processing of employee data. Furthermore, Telenor ASA claims that there is no ambiguity regarding the processing of customer data, 'which is mainly carried out by Telenor ASA's various subsidiaries as telecom operators, and where Telenor ASA's role in this, if any, is primarily as processor through Telenor Research and GIAI'.[55]

[51] Telenor ASA's Article 30 record of 2 February 2022
[52] Telenor ASA's Article 30 record of 2 February 2022
[53] '2021.09.09 – TNASA Privacy status and proposals for GU Forum.pdf', p. 13.
[54] '2021.09.09 – TNASA Privacy status and proposals for GU Forum.pdf', p. 14.
[55] 'Preliminary inspection report – With comments from Telenor ASA in yellow', 16 May 2022, p. 8.

Datatilsynet has no basis for determining that the statement from the external DPO applies to customer data, but cannot see how the description can possibly only concern employee data in Telenor ASA. The concern relates to the sharing of personal data between 'Business Units' in the Telenor Group. Telenor ASA has not presented any arguments or documentation to support the claim that the general description above applies to employee data. Regardless of the personal data in question, it appears that the division of responsibility has been unclear.

Furthermore, the external DPO has expressed the following in an email correspondence in the context of Schrems II issues, which shows concern with regard to the division of controllership in general:

- 'In my opinion, for initiatives rolled out by, or directed by ASA, ASA should be regarded a "data controller" under the law and through that will have several obligations to adhere to which cannot simply be outsourced. That is not to say that some concrete activities may not be outsourced, but privacy accountability cannot, and consequently a not insignificant level of involvement by ASA business-, system- and contract owners will be required regardless of outsourcing. Put differently, as long as ASA has an operational involvement in business activities involving processing of personal data, whether it's within ASA itself or exercised upon other businesses through ASAs role as HQ, there are privacy obligations to adhere to that ASA cannot fully escape. With that said, I am of course looking forward to Group Legal's assessment on this topic!
- Currently, there seems to be a dilution of responsibility between the entities mentioned, where no single party takes full responsibility of privacy issues/activities or is even capable of doing it. For example:
    - BUs may be struggling with the conundrum of being "accountable for their own privacy", while at the same time being required to adopt what comes down the pipe from ASA/GSS/TPC and themselves being unable to impact product/system features, contracts or even privacy assessments – and expecting that things they are directed to do business wise has been properly checked out privacy wise, which is often not the case;
    - GSS may be expected to implement systems and features as prescribed by a business owner at ASA, even potentially impacting data flows or data access of other BUs or between ASA/BUs, but where GSS is lacking ownership, involvement or access to assessments or contracts/frameworks enabling this;
    - TPC may be entering into contracts under their mandate, which then typically has a commercial focus and an inadequate privacy focus, impacting all later (privacy) activity down the chain;
    - ASA does not have (my opinion) the proper awareness, competence and/or resources to do necessary compliance work with sufficient quality and timeliness (including catching up with backlog), on behalf of itself or group

> initiatives that other BUs must rely upon. There are simply things falling through the cracks with how things are currently set up.'[56]

Telenor ASA has pointed out that the first paragraph in the citation specifically relates to a potential outsourcing of certain operational privacy-related tasks in Telenor ASA to Telenor Global Shared Services (GSS), which has not been carried out to date. Telenor ASA therefore is of the opinion that the first paragraph is not relevant to the inspection, and that these general concerns have been followed up in dialogue between the DPO and management.[57] Even if the email was sent in that context, it is necessary to look at the wording. The wording he uses is 'for initiatives rolled out by, or directed by ASA'. Datatilsynet therefore finds the statement relevant, as it reflects a concern with regard to understanding the division of responsibilities for different processing activities, even if the specific outsourcing was not carried out.

Telenor ASA does not consider our mentioning in the inspection report of Telenor ASA's processing of customer data to be a suitable description of its actual processing activities.[58] We have written the report and advance notification of the decision based on the documents submitted, including information provided in the record of processing activities and in interviews. If the descriptions are still not accurate, this is due to the fact that information previously received from the company has been inadequate or incorrect. We note that it was not until the case culminated in the notification of the decision that we received more detailed information in the company's response.

In its comments on the advance notification, Telenor claims that Telenor ASA does not process large amounts of customer data and/or personal data of a more intrusive nature as processor, despite the fact that our opinion is based on the descriptions in their record of processing activities.

In its comments on the advance notification, Telenor ASA states that:

> 'In this system, there are certain standardised and partly pre-filled text boxes and hashtags that the person who fills in the record chooses from, which in certain cases may lead to the contents of the protocol being misunderstood/filled in incorrectly, for example in the indication of who the data subjects are, the number of data subjects, the types of personal data being processed etc. In retrospect, Telenor acknowledges that there are such sources of misunderstandings and errors in the document that has been submitted to Datatilsynet. For example, the company acknowledges that figures have been given for a number of items that may leave the impression that personal data processing takes place on a larger scale and of a more extensive scope than is actually the case. Based on the indication of the types of data being processed, it is in some places easy to misunderstand what the processing actually concerns and the type of information involved. There are also other aspects of the actual setup used that the

[56] From email correspondence 'Mail to EVP People', 13 April 2021.
[57] 'Preliminary inspection report – With comments from Telenor ASA in yellow', 16 May 2022, p. 9.
[58] Comments on the advance notification of 31 May 2024, pp. 16–17.

> company acknowledges has affected the content of the submitted material in a way that can lead to incorrect conclusions or misunderstandings. It is therefore unfortunate that Datatilsynet has relied on a literal interpretation of the content, without taking into account Telenor's attempt to explain the facts that form the basis for the extraction.'[59]

As mentioned above, it is Telenor ASA's responsibility, as controller and processor, to ensure that the record of processing activities is completed and up to date. This includes ensuring that the information is correct. The company must expect Datatilsynet to rely on and base its decision on the content of the submitted record of processing activities. That is the very purpose of a record of processing activities cf. GDPR recital 82:

> 'In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations.'

If the company itself considers that the record of processing activities was, and still is, misleading, it falls within the obligation set out in Article 30, supplemented by Article 24, to ensure that the record of processing activities is revised and updated. If the content has deficiencies because different people have lacked the competence required to complete the record or the solution used is not suitable. Telenor ASA should have ensured to have procedures or follow-up measures in place, or other appropriate organisational and technical measures to ensure that the record is as up to date and correct as possible. If information is available in other more suitable systems, we expect this to have been forwarded along with the response.

We note that the response provides more detailed information. This is useful, but in our opinion, this shows that the processing activities referred to are of a significant scope and that Telenor ASA's processing activities are not limited to simple HR management for employees of Telenor ASA. Again, this information confirms that the company also acts as joint controller and as processor, and not only as controller. This must be included in the assessment of, among other things, whether the company is obliged to have a DPO. It also emerges in the response that Telenor ASA processes customer data to some extent when they write: 'it is *essentially* the mobile companies in the Telenor Group that process data related to external customers, and not Telenor ASA'[60] (our italics).

We also remind you that whether an enterprise acts as controller, joint controller and/or processor depends on the actual circumstances and not on formal roles.[61] Regardless of which group structure Telenor has chosen and what role is defined for Telenor ASA, it is the actual

---

[59] Comments on the advance notification of 31 May 2024, p. 13.
[60] Comments on the advance notification of 31 May 2024, p. 10.
[61] See for example CJEU case C-638/21 *NVSC* ECLI:EU:C:2023:949 paragraphs 29–31. See also EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 2.0 adopted on 7 July 2021 Section 12: 'The concepts of controller and processor are functional concepts: they aim to allocate responsibilities according to the actual roles of the parties.'

circumstances in the company and its relationship with its subsidiaries that must be used as a basis.

5.2.4 **Regarding contact information**

On the day of the inspection, we were unable to find contact information for Telenor ASA's DPO on Telenor's website. Telenor ASA explained that the contact details were available on the intranet for employees since the majority of personal data processing concerns employees and internal relations.[62] This has not been verified, but we assume that it was known to the employees who Telenor ASA's DPO was and how to make contact with that person.

Datatilsynet notes that it is of utmost importance that *all* data subjects, internal and external, have easy access to the contact details of the company's DPO, regardless of whether the company acts as controller or processor. We regard this as a precondition for being able to safeguard the data subject's rights set out in Article 38(4) GDPR. Therefore, the DPO's contact information should be published for example on the company's website, and it should be clear that the receiver of the emails to that address is in fact the DPO. For example, a generic email address to customer service would not be satisfactory in our opinion.

Our assessment is that this constitutes a partial violation of Article 37(7) GDPR, but we otherwise find Telenor ASA to be in compliance with Article 37 GDPR, within the scope of the inspection. We note that Telenor ASA updated the online privacy statement on 3 February 2022 with the DPO's contact details.[63]

5.2.5 **Conclusion**

The inspection has uncovered unclear and incomplete records of processing activities at Telenor ASA and ambiguities that need to be resolved regarding, among other things, Telenor ASA's responsibility for certain processing activities, categories of personal data and the number of data subjects. The record of processing activities must be made available to Datatilsynet on request, cf. Article 30(4) GDPR and Recital 82 GDPR. This means that the company must be aware of the importance of maintaining the record and that it can and will be used as evidence in connection with an inspection.

Based on Telenor ASA's processing activities, as described above, we are of the opinion that it is not obvious that the company is not obliged to have a DPO. This must first be seen in conjunction with the company's role as controller, joint controller and processor, respectively, and secondly with what these activities actually entail. Telenor ASA must therefore consider whether it is obliged to have a DPO and document this assessment before a conclusion can be made.

---

[62] 'Preliminary inspection report – With comments from Telenor ASA in yellow', 16 May 2022, p. 3.
[63] http://www.telenor.com/privacy-policy/

6 Involvement of the data protection officer – Article 38(1) GDPR

6.1 Inspection criteria and evidence

Article 38(1) GDPR reads as follows:

'The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.'

Furthermore, when carrying out a data protection impact assessment (DPIA), the controller has a specified obligation to seek the advice of the DPO pursuant to Article 35(2) GDPR. We further refer to sections 3.2.1 and 3.2.2 in the final inspection report of 30 September 2022.

6.2 Datatilsynet's assessment

According to the wording of Article 38(1) GDPR, the DPO shall be involved 'properly' and 'in a timely manner' in all data protection issues. These requirements demand a proportionality assessment, as what is 'properly' and a 'timely manner' will vary depending on the complexity and nature of the relevant data protection issues. This requires the controller to have appropriate measures in place, e.g. internal procedures, to ensure that the involvement of the DPO meets the requirements of Article 38(1) GDPR. Without any form of internal, documented standard procedures, it will be difficult for the employees to evaluate what is 'properly' and 'timely' in each situation.

The Guidelines on Data Protection Officers from the former Article 29 Data Protection Working Party (WP29), which were endorsed by the European Data Protection Board (EDPB), set out examples of what enterprises should do to comply with the provision at hand:

> '[…] the organisation should ensure, for example, that:
>
> - The DPO is invited to participate regularly in meetings of senior and middle management.
> - His or her presence is recommended where decisions with data protection implications are taken. All relevant information must be passed on to the DPO in a timely manner in order to allow him or her to provide adequate advice.
> - The opinion of the DPO must always be given due weight. In case of disagreement, the WP29 recommends, as good practice, to document the reasons for not following the DPO's advice.
> - The DPO must be promptly consulted once a data breach or another incident has occurred.
>
> Where appropriate, the controller or processor could develop data protection guidelines or programmes that set out when the DPO must be consulted.'[64]

[64] WP 243 rev.01 'Guidelines on Data Protection Officers', p. 14.

The EDPB's guidelines are not binding, but set out elements that are relevant in an assessment of whether an organisation complies with Article 38(1) GDPR. The EDPB's guidelines reflect the common understanding and practice of the EEA's data protection supervisory authorities. They are therefore a relevant source for interpreting the GDPR, in particular in view of ensuring consistent application of the GDPR across the EEA, as required by Articles 51(2) and 70(1) GDPR.[65]

The Telenor Group's Group Privacy Policy prescribes that each company within the group (Business Units):

> 'shall appoint a Data Protection Officer who advises and reports on privacy matters to the top level of management in the Business Unit […]'.[66]

The Telenor Group's Group Manual Privacy Policy states that the DPO must:

> '[a]dvise management and personnel in the Business Unit on risks and best practices related to processing of personal data, including the resources needed and effort required in order to manage privacy risk in the processing activities of the Business Unit and the privacy impact of processing activities'.[67]

These two internal documents set out overarching obligations on a general level for all companies within the group, including Telenor ASA.

Pursuant to the Group Privacy Manual, a data protection impact assessment (DPIA) should as a minimum:

> '[i]nclude an independent recommendation from the DPO before the assessment is concluded'.[68]

Furthermore, in the event of privacy incidents, the DPO should as a minimum:

> 'be consulted for his/her independent opinion on assessments of the breach impact and the risk it poses to the individuals, as well as the effect of mitigating controls in limiting the incident'.[69]

Other than what follows from the above-mentioned general internal requirements for all companies in the Telenor Group, Datatilsynet was not provided with any written procedures during the inspection or with other standard policies specifically for Telenor ASA regarding the timing and manner for involving Telenor ASA's DPO in all issues related to the protection of personal data.

---

[65] See GDPR Recitals 10, 123 and 139.
[66] 'Group Privacy Policy, valid from: 2022-01-01', p. 1.
[67] 'Group Privacy Manual, valid from: 2022-01-01' p. 1.
[68] 'Group Privacy Manual, valid from: 2022-01-01' p. 6.
[69] 'Group Privacy Manual, valid from: 2022-01-01' p. 8.

The only internal standard process for involving the DPO we have identified during the inspection consists in having regular meetings between the DPO and functions in the line organisation, i.e. through the Group Unit Forum (GU Forum) and meetings with Privacy Coordinators in the line organisation. However, these regular meetings are a result of recent developments, as set out below.

Telenor ASA's DPO started attending meetings of the GU Forum in September 2021.[70] While involvement of the DPO requires the line organisation to reach out to the DPO for their advice on arising issues, the main purpose of the DPO's participation in the GU Forum was to establish a proper DPO reporting line:

> '… [the CEO] agreed that it would be useful to delegate the authority of privacy reporting from the DPO in Telenor ASA, from [the CEO], to the Policy owner and Group Unit forum'.[71]

Prior to attending meetings of the GU Forum, the DPO was able to attend Compliance Committee Meetings (CCM), but did not regularly attend these meetings. The meetings were less suitable for the involvement of the DPO, since the meetings were limited to handling issues in the Telenor Group and not dedicated specifically to data protection issues; see section 3.5.2 in the final inspection report of 30 September 2022.

The Privacy Coordinators in the different units in Telenor ASA's line organisation have meetings with the DPO on a weekly basis, at which they can discuss data protection issues.[72] The external DPO[73] mentioned in the interview that getting all the Privacy Coordinators in the different Group Units in place had been crucial. Furthermore, he stated that, before the appointment of these coordinators, the DPO did not have sufficient links out to all the different parts of the company.[74]

Telenor ASA has stated that the DPO has regular meetings with Group Legal and the temporarily hired Schrems II resource, and that at these meetings it is possible to exchange information.[75] Datatilsynet has not been provided with any documents that formalise the occurrence of such regular meetings.

Other than the above-mentioned regular meetings, the involvement of Telenor ASA's DPO in issues that relate to the protection of personal data takes place on a case-by case basis.[76] The same occurred before these regular meetings were established. The final inspection report shows how the case-by-case involvement is carried out.[77] There appears to have been some ad hoc involvement of the DPO in data protection matters in the period between October 2020

[70] Final inspection report of 30 September 2022, p. 20.
[71] Email where the CEO delegates responsibility for the DPO's reporting.
[72] Interview with the DPO of Telenor ASA and the Privacy Coordinators
[73] 'The external DPO' refers to the DPO who was hired from [redacted] during the period January 2021 to October 2021, cf. the final inspection report of 30 September, p. 2.
[74] Final inspection report of 30 September 2022, p. 13.
[75] Final inspection report of 30 September 2022, p. 3.
[76] «Response to Datatilsynet», 13 December 2021 p. 8.
[77] Final inspection report of 30 September 2022, pp. 3–4.

and January 2022. However, due to the informal nature of the involvement, it is difficult for Datatilsynet to conclude on the exact extent to which Telenor ASA's DPO has been involved in 'all issues which relate to the protection of personal data', cf. Article 38(1) GDPR.

Even though we find that there has been a risk of Telenor ASA's DPO not being involved in all issues related to the protection of personal data 'properly' and 'in a timely manner', we do not conclude that Article 38(1) GDPR has been violated in the timeframe of the inspection, as there is no preponderance of evidence. We find a lack of policies to clarify in which cases and how the DPO should be involved. See section 12.2 on the legal requirements of Article 24(1) and (2) GDPR to implement organisational measures and appropriate data protection policies, which entails sufficient and clear content.

7 Allocation of resources – Article 38(2) GDPR

7.1 Inspection criteria and evidence

Article 38(2) GDPR reads as follows:

> 'The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.'

We further refer to sections 3.3.1 and 3.3.2 in the final inspection report of 30 September 2022.

Pursuant to Article 39(2) GDPR:

> 'The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.'

We refer to section 3.8 in the final inspection report regarding the DPO's tasks mentioned in Article 39.

7.2 Datatilsynet's assessment

The requirement to provide necessary resources for the DPO to carry out their tasks is a general and overarching requirement. In addition, Article 38(2) GDPR sets out an obligation to give the DPO access to personal data and processing operations, and to facilitate the maintenance of their expert knowledge.

Pursuant to Article 39 GDPR the DPO has the task of informing and advising the controller or the processor, and monitor the compliance with the GDPR. A clarification of Telenor ASAs role is therefore important when assessing whether the DPO has been allocated sufficient resources to carry out their tasks.

The Guidelines on Data Protection Officers from the former Article 29 Working Party provide guidance on what should be done to fulfil the requirements in Article 38(2) GDPR:

> 'The following items, in particular, are to be considered:
>
> - Active support of the DPO's function by senior management (such as at board level).
> - Sufficient time for DPOs to fulfil their duties. This is particularly important where an internal DPO is appointed on a part-time basis or where the external DPO carries out data protection in addition to other duties. Otherwise, conflicting priorities could result in the DPO's duties being neglected. Having sufficient time to devote to DPO tasks is paramount. It is a good practice to establish a percentage of time for the DPO function where it is not performed on a full-time basis. It is also good practice to determine the time needed to carry out the function, the appropriate level of priority for DPO duties, and for the DPO (or the organisation) to draw up a work plan.
> - Adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate.
> - Official communication of the designation of the DPO to all staff to ensure that their existence and function are known within the organisation.
> - Necessary access to other services, such as Human Resources, legal, IT, security, etc., so that DPOs can receive essential support, input and information from those other services.
> - Continuous training. DPOs must be given the opportunity to stay up to date with regard to developments within the field of data protection. The aim should be to constantly increase the level of expertise of DPOs and they should be encouraged to participate in training courses on data protection and other forms of professional development, such as participation in privacy fora, workshops, etc.
> - Given the size and structure of the organisation, it may be necessary to set up a DPO team (a DPO and his/her staff). In such cases, the internal structure of the team and the tasks and responsibilities of each of its members should be clearly drawn up. Similarly, when the function of the DPO is exercised by an external service provider, a team of individuals working for that entity may effectively carry out the tasks of a DPO as a team, under the responsibility of a designated lead contact for the client.
>
> In general, the more complex and/or sensitive the processing operations, the more resources must be given to the DPO. The data protection function must be effective and sufficiently well-resourced in relation to the data processing being carried out.'[78]

While the guidelines are not binding, they set out relevant factors for assessing whether an organisation complies with the requirements in Article 38(2) GDPR.

[78] WP 243 rev.01 'Guidelines on Data Protection Officers' adopted 13 December 2016, p. 15.

We further refer to the final inspection report of 30 September 2022, pp. 10–11, for the factual background.

Sufficient time for the data protection officer to perform tasks

Allocating sufficient time for the DPO to perform their tasks is one of the main factors to ensure compliance with Article 38(2) GDPR.

Telenor ASA's DPO[79] is appointed in a 50 per cent FTE (Full-Time Equivalent) position, while the remaining 50 per cent is in principle allocated to being an associate lawyer ('advokatfullmektig') in Telenor ASA's Group Legal department.[80] Telenor ASA specifies that, since October 2020, the DPO has in practice spent most of their working hours on performing tasks connected to the DPO role.[81] However, this was not formalised in any document shared by Telenor ASA with Datatilsynet. It has been pointed out on several occasions and from different people that, in practice, the allocation of a 50 per cent FTE for the DPO neither is nor has been sufficient in practice.[82]

Furthermore, several circumstances indicate that even the above-mentioned practical increase of the time spent working on DPO tasks has not been sufficient. Based on the documentation we received, there was a major backlog in the first half of 2021,[83] which also indicates that the DPO did not have sufficient time to perform their tasks. In this regard, the external DPO noted in September 2021 that the 'DPO spends 50% more time than originally intended, while still being overburdened with tasks and being a bottleneck' and that '[m]ost time [is] spent on retro-active issue management, instead of pro-active and strategic work'.[84] This indicates a lack of resources as regards the DPO being able to perform their tasks.

Telenor ASA's management stated that they would look into whether there is a need to formally allocate a 100 per cent FTE to Telenor's DPO.[85] We find that having a 50 per cent FTE as a flexible, informal resource allocation may result in conflicting priorities, when the allocation of (at least) a 100 per cent FTE seems necessary.

Telenor ASA's DPO mentioned in the interview that she assumes that a 50 per cent FTE will be appropriate with time, but that it will require another level of data protection maturity compared with the current state of affairs.[86]

Furthermore, the interview revealed that the DPO planned to acquire a licence as a lawyer, which would require practical procedural experience from legal matters as well as taking legal

[79] 'The DPO' refers to the DPO at the time of the inspection, also referred to as the 'then DPO' in the document, even though they no longer hold this role. Elsewhere, 'the DPO' refers to the role, regardless of whether it is the external or the current DPO.
[80] 'Response to Datatilsynet', 13 December 2021, p. 10.
[81] Final inspection report of 30 September 2022, p. 11.
[82] Final inspection report of 30 September 2022, p. 11.
[83] '2021.04.13 – Mail to EVP People'. '2021.09.09 – TNASA Privacy status and proposals for GU Forum.pdf'.
[84] '2021.09.09 – TNASA Privacy status and proposals for GU Forum.pdf', p. 14.
[85] Final inspection report of 30 September 2022, p. 11.
[86] Final inspection report of 30 September 2022, p. 11.

courses. Telenor planned to facilitate this procedural experience, and it would presumably take place within working hours.[87] Telenor ASA has stated that the formal requirements to obtain the licence will be fulfilled over time depending on the amount of court cases, and that obtaining the procedural experience might take several years. Furthermore, it will mainly encompass smaller cases relating to the business of Telenor Norge AS.[88]

Reports from the data protection officer on the resource situation

On several occasions in 2021 and 2022, the DPO raised concerns about the need for more resources.[89] For instance, in February 2021, the DPO recommended the continued allocation of:

> '100% FTE on ASA privacy matters (50% DPO, 50% extra) until privacy org./compliance state more mature'.[90]

At the first meeting of the GU Forum in September 2021, the DPO reported the following:

- 'DPO spends 50% more time than originally intended, while still being overburdened with tasks and being a bottleneck [+P]
- Most time spent on retro-active issue management, instead of pro-active and strategic work [+I/P]
- Internal alignment between CM, BSO and DPO delayed due to capacity and prio [+I/P]
- High-risk processing activities uncovered which should have had a DPIA, but did not (e.g. recording, investigations, tutela) [+I/P]
- Lack of capacity to deal (properly) with known cases [+P]
- Lack of audits and follow-up of contracts makes it a guessing game to assess whether 3rd parties are complying [+I/P]
- Lack of capacity and competence to follow-up systematically [+I/P]'[91]

In and of itself, these reports from the DPO are factors showing a lack of resources.

In its letter of 16 May 2022, Telenor states that the need for more resources flagged by the DPO has been taken on board by the management, which has been documented.

Conclusion

The inspection has uncovered that the formal allocation of a 50 per cent FTE for the DPO has not been sufficient. Furthermore, several circumstances indicate that even dedicating most of the working hours of one person to the performance of DPO tasks has not been sufficient. We emphasise that the DPO can hardly perform all the tasks listed in Article 39 GDPR without being provided with the necessary resources by the employer pursuant to Article 38(2) GDPR.

---

[87] Final inspection report of 30 September 2022, pp. 10– 11.
[88] Interviews with [redacted] DPO of Telenor ASA and the manager of Group Legal. 'Preliminary inspection report – With comments from Telenor ASA in yellow', 16 May 2022, p. 10.
[89] Final inspection report of 30 September 2022, pp. 8–10, 15–16.
[90] Final inspection report of 30 September 2022, p. 10.
[91] Final inspection report of 30 September 2022, pp. 15–16.

Throughout 2021 and 2022, Telenor ASA has put in place more support functions and resource allocation for facilitating the fulfilment of the DPO's tasks. This was a positive change during the timeframe of the inspection.

Based on the above, there was a backlog and a general diffusion of responsibility and accountability, with many specific data protection issues that needed the attention and involvement of the DPO.[92] The increase of resources (financial privacy/compliance budget and adding privacy coordinators) may indirectly support the DPO role, but are not allocated specifically to ensuring that the DPO is able to perform their tasks.

Datatilsynet finds that Telenor's DPO has been supported with the necessary resources to facilitate the maintenance of their expert knowledge.

In an overall assessment based on the available documentation, interviews and information provided in response to the advance notification, Datatilsynet finds under doubt that there is a preponderance of evidence that Telenor ASA has violated Article 38(2) GDPR by not providing the DPO with the resources necessary to perform the tasks referred to in Article 39 within the timeframe of the inspection.

8 The data protection officer's access to the highest management – Article 38(3)

8.1 Inspection criteria and evidence

The last sentence of Article 38(3) GDPR reads as follows:

> 'The data protection officer shall directly report to the highest management level of the controller or the processor.'

We further refer to sections 3.5.1 and 3.5.2 in the final inspection report of 30 September 2022.

8.2 Datatilsynet's assessment

Under Article 38(3) GDPR, the controller shall ensure that the DPO directly reports to 'the highest management level'. The use of the word 'highest' – as a superlative to 'high' – indicates that the DPO is to report directly to the absolute top level of management of the relevant controller or processor. What is considered the top level of management will depend on the form of incorporation and the organisational structure in each specific case.

Furthermore, when interpreting a provision of EU law, it is necessary to consider not only its wording but also its context and the objectives of the legislation it forms part of.[93] Therefore, the preparatory works of Article 38(3) GDPR should be taken into account to consider its proper interpretation.[94]

---

[92] See section 5.2.3.
[93] CJEU Case C-505/19, EU:C:2021:376, paragraph 77.
[94] See *inter alia* CJEU case C-621/18, *Wightman and Others,* judgment of 10 December 2018 (EU:C:2018:999), para 47; case C-548/18, *BGL BNP Paribas*, judgment of 9 October 2019 (ECLI:EU:C:2019:848), para 25.

The legislative process that led to the adoption of Article 38(3) GDPR supports the conclusion that the DPO must report directly to the absolute top management of the relevant organisation. In the European Commission's initial draft of the GDPR, it was set out that the DPO must report to 'the management', without specifying the management level to which the reporting should be addressed.[95] The European Parliament suggested replacing the word 'management' with 'executive management'.[96] The European Parliament also added – as an additional safeguard – that there should be a dedicated executive management member responsible for GDPR compliance.[97]

The wording of Article 38(3) was further amended by the European Council, and it was proposed to specify that the reporting should be addressed to the 'highest management'.[98] The Council's approach was ultimately embraced in the final version of the Regulation.

Emphasis is put on specifying the management level to which the reporting should be addressed to ensure that the highest management level of the relevant organisation is kept informed and involved in how the company complies with the GDPR and its own internal procedures, and is thus able to intervene to ensure that the measures that are necessary to ensure compliance are put in place.[99] The reference to the highest management level must also be seen in the context of the accountability principle in Article 5(2) GDPR, where the controller is responsible for demonstrating compliance with the provision.

In this regard, it should be noted that the WP29 Guidelines on Data Protection Officers ('DPOs') state that:

> '[...] Article 38(3) [provides] that the DPO "shall directly report to the highest management level of the controller or the processor". Such direct reporting ensures that senior management (e.g. board of directors) is aware of the DPO's advice and

[95] See the European Commission's initial draft of the GDPR (COM/2012/011 final – 2012/0011 (COD)), dated 25 January 2012, where Article 36(2) (today's Article 38(3)) states: '[…] The data protection officer shall directly report to the management of the controller or the processor.' The problem of a potential conflict of interest arising as a result of the reporting line being situated on too low a level in the company's hierarchy was not addressed.

[96] See the draft of the GDPR adopted by the European Parliament (EP-PE_TC1-COD(2012)0011), dated 12 March 2014, where Article 36(2) (today's Article 38(3)) states: '[...] The data protection officer shall directly report to the executive management of the controller or the processor.'

[97] Ibid. See Article 36(2) (today's Article 38(3)) last sentence, which states: 'The controller or processor shall for this purpose designate an executive management member who shall be responsible for the compliance with the provisions of this Regulation.'

[98] See the draft of the GDPR adopted by the European Parliament (5419/1/16 REV 1), dated 8 April 2016, where Article 38(3) states: 'The data protection officer shall directly report to the *highest management level* of the controller or the processor' (emphasis added). With this amendment of the specification of the management level, the Council decided to remove the European Parliament's suggestion to dedicate an executive member of management to be responsible for compliance with the provision.

[99] Åste Marie Bergseng Skullerud, Cecilie Rønnevik, Jørgen Skorstad and Marius Engh Pellerud: *Personopplysningsloven og personvernforordningen (GDPR), kommentarutgave* (2019) p. 344.

> recommendations as part of the DPO's mission to inform and advise the controller or the processor.'[100]

The reference to the 'board of directors' as an example of the highest management must be considered in light of the organisational structure of the controller or processer on a case-by-case basis. Not all controllers or processors would have a board of directors. For example, public authorities and organisations such as municipalities, counties, universities, schools, governmental bodies etc. would typically not have a board of directors as the highest level management. The example provided in the WP29 Guidelines must therefore be understood as a specific example of the highest management, which applies in those situations where such a form of management organisation is compulsory (typically for private limited companies and public companies), or simply where this form of management structure is chosen independently of any compulsory requirements.

In the present case, Telenor ASA is organised as a public limited liability company subject to the Norwegian Public Limited Liability Companies Act. The company is obliged to have a board of directors (board).[101] This is also apparent from Telenor ASA's organisational chart.[102]

In its comments on the advance notification of 31 May 2024, Telenor ASA states that:

> 'No specific requirements can be set for who should be reported to, or how reporting should take place.'
>
> 'that the reporting structure and format are adapted to the individual company's "size, organisation and current risk picture", so that the controller has "flexibility" with regard to the reporting line.'[103]

Datatilsynet emphasises that, it is the company's responsibility to specify what constitutes reporting to the highest level. Precisely because the 'highest management level' is not always clear, it is all the more important to have a clear and documented reporting line as regards whom the DPO should report to and how. We will return to this in section 12.2 on Article 24.

In this case, it is assessed whether Telenor ASA has put in place measures to ensure that its DPO reports directly to Telenor ASA's highest management level.

Several measures may be relevant to ensure compliance with Article 38(3) GDPR.[104] In our view, it is essential to formalise and explain the DPO's reporting line (in internal documents,

---

[100] WP 243 rev.01 'Guidelines on Data Protection Officers' adopted 13 December 2016, p. 15.
[101] Act of 13 June 1997 on public limited liability companies (Public Limited Liability Companies Act), Sections 6-1 and 6-12.
[102] https://www.telenor.com/about/corporate-governance/board-of-directors/
[103] Comments on the advance notification of 31 May 2024, p. 36.
[104] See CNPD (Luxembourg Data Protection Authority) – Decision No 41 FR/2021 (Délibération N° 41FR/2021 du 27 octobre 2021 – mesure correctrice et amende), paragraph 68, where the CNPD, in its assessment of Article 38(3), noted that: 'Several measures can be considered to achieve this result, such as linking the DPO to the top management level to ensure maximum autonomy [for the DPO] or creating a formalised and regular direct

such as policies, procedures, instructions, job descriptions etc.), and make sure that the DPO reports to the highest management in practice.

Between 2020 and 2022, Telenor ASA introduced several amendments to its formal procedures, practices and policies for DPO reporting.[105] During the interviews conducted in connection with our inspection, Telenor ASA took the view that, throughout this period, there were measures in place to ensure that the DPO reported directly to the organisation's highest management. This view is further expressed in Telenor ASA's comments on the preliminary inspection report, in which they write:

> 'Furthermore, the role of DPO reports to top management and local policy owner [redacted] through the GU Forum and otherwise as the DPO finds necessary.'[106]

Based on the findings of our inspection, we find that Telenor ASA's statement should be rejected in the present case for the whole timeframe of the inspection. The reasons for this are outlined below.

Firstly, it must be examined how the top management's responsibility for compliance with the requirements of Article 5(2) GDPR is formalised.[107] The functional job description for Telenor's DPO is as follows:

> 'As DPO for Telenor ASA report directly to the highest management level of the Telenor ASA on the status of data protection and urgent matters.'[108]

This wording merely mirrors the wording of Article 38(3) and does not demonstrate the existence of any direct relationship between the DPO and the highest level of management of Telenor ASA. Furthermore, it is not specified what is meant by 'highest management level' in this context. A mere reference in the job description to the fact that the DPO shall report directly to the highest management is not sufficient to ensure compliance with Article 38(3). We expect organisational measures to be in place regarding where, when, how and to whom exactly the DPO shall report in documented internal data protection policies. This is particularly important when Telenor ASA now claims that it cannot be understood to mean that the DPO should report to the company's board of directors.[109] The understanding of what constitutes the 'highest management level' must be specified.

The board is officially the highest level of Telenor ASA. Without further clarification of the reporting line, it is therefore reasonable to assume that it is the board that constitutes the 'highest management level.' Telenor ASA points out in its response, it is not clear under the

---

reporting line, as well as an escalation mechanism for urgent matters to management that can bypass the intermediate hierarchical level(s).' (our translation from French to English).

[105] Final inspection report of 30 September 2022, section 3.5.2.

[106] 'Preliminary inspection report – With comments from Telenor ASA in yellow', 16 May 2022, pp. 15–16.

[107] See also CNPD (Luxembourg) – Decision 41FR/2021, paragraphs 41 and 42.

[108] 'DPO – Functional Job Description – Group Legal – Associate Lawyer & DPO'

[109] In its comments on the advance notification of 31 May 2024, p. 37, Telenor ASA states: 'There is *no basis for (i) requiring the DPO to report to the company's board of directors*; or for (ii) requiring the controller to have formalised policies on how and to whom the DPO reports.' (our italics).

GDPR that the highest level of management must be the board of directors. In its response, Telenor ASA refers to the annotated edition of Jarbekk et al., which states that the DPO should not report to the board because the board only reports to the general manager, and that 'there is nothing to indicate that the DPO is supposed to be on equal footing with the general manager vis-à-vis the board'.[110] Here, we point out that the EDPB has a different interpretation, and that the preparatory works to the GDPRshow that the intention is precisely that the DPO should be able to report to what is de facto the highest management level in a company. These are sources of law that we assess having greater weight than legal theory. How this is in keeping with Norwegian company law is not mentioned in the preparatory works to the Norwegian Personal Data Act. The intention is to ensure the DPO's independence, and the DPO must thus be able to report and give advice independently of the company's formal line organisation.

The DPO is closely linked to the accountability principle in Article 5(2) GDPR.[111] The DPO is a role based on 'authority and expertise rather than on formal powers over the governance of personal data within organisations'.[112] The DPO has no formal role vis-à-vis the board and has no authority that goes beyond the company's, but has an independent advisory and overseeing role with 'expert-based autonomy'.[113] There may be cases where it is necessary to alert the board of privacy risks in the company. The board shall ensure that the business activities are soundly organised, cf. the Public Limited Liability Companies Act Section 6-12(1) and shall supervise the day-to-day management and the company's activities in general, cf. same law Section 6-13(1). The responsibility under Article 5(2) GDPR thus formally rests with the board, even if day-to-day data controllership is assigned to others in the company.

Jarbekk et al. also write that the highest level does not necessarily mean *the top manager*, but the highest level of day-to-day management. The general manager is responsible for the day-to-day management of the activities of a public limited company, cf. the Public Limited Liability Companies Act Section 6-14. In Telenor ASA's case, the highest level of day-to-day management is the CEO or CEO with the management team (Group Leadership Team). If we rely on this understanding of the highest level, it would be natural for the DPO to report to the CEO or CEO with the Group Leadership Team. It can be argued that such interpretation safeguards the purpose of the provision, as the top day-to-day management will be the closest to take action on basis of the DPO's report, precisely because they are exercising operational management in the company on a daily basis.

The response also refers to how Jarbekk et al. emphasise that there is some flexibility in the exact reporting lines, but does not specify whether this means that the reporting can be made to levels below the highest level of management.[114] Such an understanding will go beyond what is possible to infer from the wording and intention of the law, which, by specifying the highest management level, clearly dictates that reporting shall be made to the highest and not

---

[110] Eva Jarbekk et al.: *Personopplysningsloven og personvernforordningen med kommentarer* (2019), p. 337
[111] Cecilia Alvarez Rigaudias and Alessandro Spina, 'Article 38 Position of the data protection officer' in Kuner, Bygrave & Docksey (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, pp. 700–708
[112] Ibid p. 701.
[113] Ibid p. 703.
[114]Eva Jarbekk et al.: *Personopplysningsloven og personvernforordningen med kommentarer* (2019) p. 337.

just any management level. We believe that such an expanded interpretation cannot be applied.

The Court of Justice of the European Union (CJEU) has stated as follows: 'As is clear from settled case-law, in interpreting a provision of EU law, it is necessary to consider not only its wording, by considering the latter's usual meaning in everyday language, but also the context in which the provision occurs and the objectives pursued by the rules of which it is part...'.[115] The highest level of management must therefore be interpreted in the light of the intention of the law, which is to 'ensure a high level of protection of natural persons within the European Union and, to that end, to ensure a consistent and homogeneous application of the rules for the protection of the fundamental rights and freedoms of such natural persons with regard to the processing of personal data throughout the European Union...'.[116]

We also point out that the reference to Voigt and Bussche in the response does not say that reporting should *not* be made to the highest level, but that it is not necessary for 'each and every routine data protection matter' to be reported to the highest management level. At the same time, they emphasise that the DPO 'must be able to report directly to the highest management level when the need arises and must not be prevented from doing so by the organisation'. In our view, the DPO can communicate with different levels of the organisation on a day-to-day basis, but should be able to report directly to the highest management level. It is important here to differentiate between Article 38(1) GDPR involvement of the DPO – which should happen on several different levels, and where the DPO is the closest to assess what is appropriate – and the formal reporting pursuant to Article 38(3) GDPR.

In Datatilsynet's view, reporting to the board fulfils the requirement pursuant to Article 38(3) GDPR last sentence. Datatilsynet is also open to that reporting to the CEO or reporting to the CEO with the concerned management may fulfil the requirement. However, such reporting requires that the DPO can escalate matters further to the board because the responsibility under Article 5(2) GDPR rests with the board, as mentioned.

It is regardless important to carry out a concrete assessment on the DPO's reporting line and document this, which we consider to be inadequate in this case. We refer to section 12 below.

It emerged in the interviews with the external DPO and the then DPO, as well as the management,[117] that the DPO reported to [redacted], Executive Vice President and Chief People and Sustainability Officer, during the first part of the inspection period. Telenor ASA realised that there was a need for broader reporting, and there were plans in place for the DPO to report to CCM (Compliance Committee Meetings).[118] Furthermore, it emerged in the interview that the external DPO made Telenor ASA aware that CCM, which was at group level, 'was probably not the optimal way of contacting management' in Telenor ASA.

[115] CJEU case C-453/21, *X-FAB Dresden*, paragraph 19 and CJEU case C-534/20 *Leistritz*, paragraph 18.
[116] CJEU case C-453/21, *X-FAB Dresden*, paragraph 25 and CJEU case C-534/20 *Leistritz*, paragraph 26.
[117] Interviews of 28 January 2022 with [redacted].
[118] See section 6.2 of the decision.

Secondly, the loan agreement between Telenor ASA and [redacted] for the hiring of the external DPO from January 2021 until October 2021 states that the DPO shall report to '[redacted], *VP Privacy and Information Management Telenor Group'*.[119] This is only a reference to the employee's line management reporting, and not to the DPO's reporting line for data protection matters.[120] [redacted] was also not responsible for compliance within Telenor ASA, but for compliance at group level.

Thirdly, Telenor ASA has a written 'Group Manual Privacy' and a 'Group Policy Privacy' for ensuring compliance within the group of companies, including Telenor ASA. During the inspection, we have received both the updated policy dated 1 January 2022 (became valid after Datatilsynet notified its inspection on 26 November 2021), and the old mandates and policies (valid between 1 June and 31 December 2021).[121] In this regard, the manual and mandate provide for some written procedures regarding the GPO's (Group Privacy Officer) reporting on data protection matters to the management, for example functionally to the Chief Compliance Officer and to the CEO through the Group Compliance Committee.[122]

Between 1 March 2020 and 30 November 2021, a group called the Group Unit for Privacy & IM worked on data protection in Telenor's Compliance department.[123] The internal document on the group's mandate states as follows:

> 'Group Privacy & IM has a preventive, advisory and supervisory role, acting independently from operational management, with particular emphasis on three main areas of responsibility:
>
> a) Act as Group Policy Manager for Privacy & IM, in accordance with Telenor's Compliance Management System to ensure that the applicable Group Manuals are kept up to date and are being effectively adopted across the Group. Group Privacy & IM shall perform core CMS activities following a Plan-Do-Check-Act model, and the implementation of the Group Manuals are subject to monitoring and management reporting, as described in chapter 4.
> b) *Act as both the Group Privacy Officer and DPO for Telenor ASA*, including the right and duty to report independently on relevant privacy risks and non-conformities to the Group President and CEO of Telenor. (Our italics).
> c) Advise and support management at the Group-level, and other key stakeholders such as Data Protection Officers (DPOs) in the BUs. Advisory and support tasks include:
>
> - Providing expertise and knowledge on specific privacy and IM topics
> - Providing expertise and input on privacy and IM advocacy activities

[119] 'DPO - [redacted] Loan staff agreement_[redacted]_DPO jan 21 - oct 21'
[120] Final inspection report of 30 September 2022, p. 17.
[121] For further details on the mandates, manuals and policies, see the final inspection report of 30 September 2022, section 5.2.2 pp. 18–19.
[122] 'Group Manual Privacy, valid from 1 June 2020', pp. 3–4, '2020 Mandate and Functional Description Group Privacy and IM (share), valid from: 01.03.2020', p. 3. In our understanding, the Group Compliance Committee is the same as 'CCM' or the Compliance Committee Meeting that Telenor ASA refers to.
[123] '2020 Mandate and Functional Description Group Privacy and IM (share), valid from: 01.03.2020'. The document was valid until 30 November 2021; see 'Response to Datatilsynet additional documentation', 10 January 2022, pp. 2–3.

- Providing expertise and input on privacy strategy and position development
- Supporting the implementation of privacy and IM requirements in relevant Group-wide processes.'[124]

It is stated that the GPO may report to the board via the Sustainability and Compliance Committee.[125] However, in its response to Datatilsynet, Telenor ASA emphasises that, despite the wording of the mandate, the roles of the DPO and the GPO were completely separate and held by two different persons.[126] Furthermore, Telenor ASA states that the reference to Group Privacy & IM acting as both the Group Privacy Officer and DPO for Telenor ASA was only meant as a reference to the DPO's organisational affiliation to that unit and that the DPO's responsibilities, tasks and reporting lines are not included in the document.[127] Telenor ASA has documented that the above positions were occupied by different individuals.[128] Datatilsynet notes that this group manual and the mandate did not then contain any specific guidelines for the DPO of Telenor ASA, which we consider to be inadequate.

Fourthly, it is our view that Telenor ASA's lack of formalised reporting lines has resulted in practical issues for the DPO in the performance of their tasks under the GDPR. During the inspection, the external DPO stated that he experienced a lack of access to the highest management level.[129] Furthermore, the external DPO emphasised that he experienced a lack of organisational efficiency and that he was frustrated because of the many hierarchical levels the DPO had to bypass and involve in order to reach the top management.[130]

In that connection, we note that the DPO's practical difficulties with bypassing hierarchical intermediaries and reporting directly to highest management level has been deemed a violation of Article 38(3) GDPR in and of itself by other supervisory authorities.[131] In its response, Telenor ASA claims that 'decisions made by a foreign supervisory authority are of little legal relevance, especially when Datatilsynet has not demonstrated that the decision constitutes an established practice'.[132] We do not agree with this claim. The GDPR applies throughout the EEA, and according to Recital 13, it aims to ensure a consistent level of protection for natural persons, ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all member states etc. We believe it is relevant to look at practices in other EEA member states since a harmonised interpretation of the GDPR is assumed to exist.

The external DPO's privacy status report and proposals for Telenor ASA in the GU Forum 2021 states:

---

[124] '2020 Mandate and Functional Description Group Privacy and IM (share), valid from: 01.03.2020', p. 2.
[125] '2020 Mandate and Functional Description Group Privacy and IM (share), valid from: 01.03.2020', p. 3.
[126] Final inspection report of 30 September 2022, pp. 17–18 and 12–13
[127] Final inspection report of 30 September 2022, p. 13.
[128] 'Preliminary inspection report – With comments from Telenor ASA in yellow', 16 May 2022, p. 11.
[129] Final inspection report of 30 September 2022, p. 18.
[130] Final inspection report of 30 September 2022, p. 18.
[131] See e.g. CNPD (Luxembourg) – Decision 20FR/2021, paragraphs 37 to 43.
[132] Comments on the advance notification of 31 May 2024 2024 p. 38.

> ‘a) DPO reporting, access & independence -The DPO is unable to perform the role effectively and independently due lack of proper implementation of the role in the organization, including clarified reporting lines, access to highest level of management and interference in reporting.’[133]

Furthermore, the following observations were made in the same report:

- ‘DPO reporting and sounding board not implemented
- Independent reporting and mgmt. access (has been) difficult’[134]

As a follow up point from the DPO, it was emphasised that Telenor ASA must:

> ‘Establish DPO reporting line to ASA mgmt.’[135]

These statements and findings from the former DPO illustrate the core issue when the controller does not ensure any formalisation of the DPO reporting line to the highest management. The external DPO did not have the option to refer to the manuals or policies to demand their right to have direct contact with highest management at the time. Rather, it was left to the DPO’s own personal initiative to involve and bypass hierarchical levels in order to reach the highest management. Thus, even though informal contact with the highest management may technically have been possible, that cannot be regarded as compliance in this case.

For the purpose of completeness, we note that Telenor ASA’s management in the interview acknowledged that only having the Privacy Policy Owner to report to was not sufficient. They saw the need for changes in the DPO’s reporting line. Thus, the management decided that the DPO should report quarterly to the CCM,[136] and from summer 2021, this reporting line was replaced by the GU Forum.[137]

In this regard, we note that the Privacy Policy Owner – i.e. [redacted] and later [redacted] – was, at the time, part of the Group Executive Management (an advisory body to the CEO) and held the titles ‘Executive Vice President and Chief People & Sustainability Officer’ and ‘Executive Vice President and Head of Strategy & External Relations’, respectively. These positions cannot be regarded as the highest management level within the meaning of Article 38(3) GDPR.

---

[133] 2021.09.09 – TNASA Privacy status and proposals for GU Forum, p. 13.
[134] ‘2021.09.09 – TNASA Privacy status and proposals for GU Forum’, p. 13.
[135] ‘2021.06.10 – TNASA Privacy status and proposals_FINAL’, p. 5.
[136] Concerning the Compliance Committee Meeting, see section 6.2.
[137] See the final inspection report of 30 September 2022, page 19, which states that the replacement of the CCM with the GU Forum was a direct consequence of the external DPO’s continued individual efforts to inform and report to management and the Privacy Policy Owner on the lack of clear and formal reporting lines to highest management level.

As regards the CCM, the external DPO pointed out that this forum was not suitable as the main reporting channel from the DPO to the highest management level of Telenor ASA.[138] These meetings were intended for addressing group level compliance issues, and privacy risks in Telenor ASA were too lightweight compared with other topics and agenda items concerning group level issues.[139] This is also illustrated by the fact that the DPO had no formal or permanent agenda slot at these meetings to present data protection matters concerning Telenor ASA.[140] If the DPO reported to the CCM, this was only on an ad hoc basis, and it was up to the DPO to ask to attend the meetings.[141] In this regard, we note that Telenor ASA has only provided minutes from *one* CCM meeting containing any information or reporting from the DPO. It is also worth mentioning that the DPO did not get an opportunity to attend in person, and the presentation prepared for CCM was circulated in writing in advance of the meeting for CCM's information and not for discussion at the meeting.[142]

The first meeting of the GU Forum attended by the DPO was held in September 2021, and data protection matters concerning Telenor ASA were on the agenda,[143] which was a positive change from CCM.

The GU Forum was established as the main arena for reporting and dialogue on data protection matters with the management of Telenor ASA.[144] The GU Forum was headed by the Executive Vice President of People & Sustainability and consisted of the heads of the other departments in Telenor ASA, called 'Group Units'.[145] In the interview, the GU Forum was described as an arena for the executive vice presidents to agree on decisions to be made in the line organisation, and the GU Forum cannot be regarded as a decision-making body in itself.[146] The GU Forum thus consists of managers in Telenor ASA, of which the Executive Vice President for Strategy & External Relations is also a member of the management team in Telenor ASA and the Group.[147]

It appears in the evidence that GU Forum is not a decision-making body.[148] This in itself indicates that GU Forum cannot be considered the highest management level in the understanding of the GDPR. Furthermore, we note that reporting to individuals in management is not the same as reporting to the management as such.

Datatilsynet notes that in a few PowerPoint presentations, Telenor ASA mentions with regard to the organisation of the data protection work that the DPO may escalate and report matters directly to 'CEO 1. escalation' and 'BoD 2. escalation' (board of directors). These are dated 6

[138] Final inspection report of 30 September 2022, p. 18.
[139] Ibid.
[140] Final inspection report of 30 September 2022, pp. 18–19.
[141] Ibid.
[142] Final inspection report of 30 September 2022, p. 18.
[143] '2021.12.03 - TNASA GU Forum re. privacy - scope and mandate_final'
[144] Ibid.
[145] 'Overview of DPO role and reporting lines', p. 2.
[146] Final inspection report of 30 September 2022, p. 20.
[147] Comments on the advance notification of 31 May 2024, p. 39.
[148] Interview with Telenor ASA's management.

December 2021, i.e. after our notification of inspection was sent.[149] This is a positive change, but we note that Telenor ASA has not submitted any information how these reporting lines work in practise. In order to meet the requirement for internal policies in Article 24(2) GDPR, we consider that the information obtained from the slides should also be recorded in the relevant policies, as the slides alone do not necessarily meet this requirement. Policies must be accessible and known in the organisation. We note that Telenor ASA, with the assistance of the DPO, made efforts to correct and improve the DPO's reporting lines to the highest management. Furthermore, the slides show that the month before we conducted the interviews, Telenor ASA had realised that there should be a reporting line to both the board and the CEO.[150] However, Telenor ASA's attempt of correction does not change the fact that, for almost a year, the DPO lacked a direct reporting line to the highest management level, as stated above.

Overall, the above circumstances have led Datatilsynet to conclude that Telenor ASA, for most of the timeframe of the inspection, did not have a direct reporting line to the highest management level and has violated Article 38(3) GDPR. See also section 3.5.3 in the final inspection report of 30 September 2022.

9 Data subjects' access to the DPO – Article 38(4)

9.1 Inspection criteria and evidence

Article 38(4) GDPR reads as follows:

> 'Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.'

We further refer to sections 3.6.1 and 3.6.2, in addition to section 3.1.2 in the final inspection report of 30 September 2022.

9.2 Datatilsynet's assessment

The objective of Article 38(4) GDPR is to establish the rights of the data subject vis-à-vis the DPO. It is closely related to Article 37(7) GDPR. We consider easy access to the DPO's contact details a precondition for the data subjects to be able to contact the DPO with regard to all privacy-related issues and concerning the exercise of their rights.

We refer to section 5.2.4 in this decision, where we point out a violation. Apart from this element, Datatilsynet did not find any indication during the inspection to suggest that this right had not been safeguarded.

---

[149] 'TNASA Privacy organisation overview', as of 2021.12.06 and '2021.09.09 – TNASA Privacy status and proposals for GU Forum.pdf'

[150] See in this context for example CNPD (Luxembourg) – Decision 20FR/2021, paragraph 39, where the restricted committee considers 'that the DPO should be able to bypass the intermediate hierarchical levels as soon as it deems necessary'.

10 Independence of the DPO and absence of conflicts of interests – Article 38(3) and (6)

10.1 Inspection criteria and evidence

The first and second sentences of Article 38(3) GDPR read as follows:

> 'The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks.'

We further refer to sections 3.4.1 and 3.4.2 in the final inspection report of 30 September 2022, in particular where it says that the external DPO informed us that he never received any direct instructions from the management regarding the exercise of his tasks. During the inspection, Datatilsynet did not find any evidence that a DPO of Telenor ASA had been dismissed or penalised by Telenor ASA for performing their tasks.

Furthermore, Article 38(6) GDPR reads as follows:

> 'The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.'

We further refer to sections 3.7.1 and 3.7.2 in the final inspection report of 30 September 2022.

10.2 Datatilsynet's assessment

In our opinion, Article 38(3) and Article 38(6) GDPR are closely related, and we therefore look at both provisions in this section.

Article 38(3) states that the controller shall ensure that the DPO does not receive any instructions regarding the exercise of their tasks. This provision is important for ensuring the independence of DPOs.[151] It refers not only to direct instructions from a superior, but also implies that a DPO must not be in a position to be inclined to accept certain compromises when dealing with the controller's staff in higher positions.[152]

[151] See Recital 97 GDPR, which states that '[…] data protection officers, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.'
[152] See by analogy the EDPS Position paper on the role of Data Protection Officers of the EU institutions and bodies (30 September 2018), p. 9.

Article 38(6) stipulates that 'the data protection officer may fulfil other tasks and duties' provided that 'any such tasks and duties do not result in a conflict of interests'.[153] It is therefore crucial that the DPO's independence is guaranteed, especially when the DPO is given other tasks in the organisation. This is because, as noted by the Network of Data Protection Officers of the EU Institutions and Bodies, a 'part-time DPO faces a permanent conflict between allocating time and efforts to their DPO tasks versus other tasks [and is] in danger of encountering conflicts of interest'.[154] It is therefore extremely important to make thorough assessments of possible conflicts of interest when establishing a part-time position as DPO.

To avoid conflicts of interests, controllers should make sure:

- 'to identify the positions which would be incompatible with the function of DPO
- to draw up internal rules to this effect in order to avoid conflicts of interests
- to include a more general explanation about conflicts of interests
- to declare that their DPO has no conflict of interests with regard to its function as a DPO, as a way of raising awareness of this requirement
- to include safeguards in the internal rules of the organization and to ensure that the vacancy notice for the position of DPO or the service contract is sufficiently precise and detailed in order to avoid a conflict of interests. In this context, it should also be borne in mind that conflicts of interests may take various forms depending on whether the DPO is recruited internally or externally.'[155]

In the present case, Telenor ASA's DPO is meant to fulfil other tasks too. As noted by Telenor ASA:

> 'The DPO is organizationally situated within the Group Legal department (a Group Unit) and has its personnel line reporting here. The DPO is appointed as a 50 % FTE position, while this person's remaining 50 % FTE is allocated to being an associate lawyer for Group Legal.'[156]

Thus, it should be assessed whether such an arrangement is compatible with Article 38(3) and (6) GDPR, and whether Telenor ASA has adopted measures to avoid possible conflicts of interests.

---

[153] WP 243 rev.01, 'Guidelines on Data Protection Officers', adopted on 13 December 2016, p. 17 (stating that: 'The absence of conflict of interests is closely linked to the requirement to act in an independent manner. Although DPOs are allowed to have other functions, they can only be entrusted with other tasks and duties provided that these do not give rise to conflicts of interests').

[154] Network of Data Protection Officers of the EU Institutions and Bodies, Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (14 October 2010), p. 6. See also the EDPS Position paper on the role of Data Protection Officers of the EU institutions and bodies (30 September 2018), p. 9.

[155] WP 243 rev.01 'Guidelines on Data Protection Officers', last revised and adopted on 5 April 2017, approved by the EDPB in Endorsement 1/2018 of 25 May 2018, p. 17.

[156] 'Response to Datatilsynet', 13 December 2021 , p. 10.

Telenor's Group Manual Privacy from 2020 states that:

> 'The BU shall ensure that the DPO is in a position to perform her or his duties and tasks in an independent manner and shall not receive any instructions regarding the exercise of these tasks. He or she shall not be dismissed or penalised by Telenor for performing his/her tasks. To avoid any conflicts of interests, the DPO cannot be organised in the line-organisation, but shall be organised in the Corporate Affairs Unit of the BU and report directly to the Corporate Affairs Officer of the BU.'[157]

In essence, the Group Manual Privacy from 2020 largely mirrors the wording of Article 38(3) and (6) GDPR, as well as Recital 97 GDPR.

The Group Policy Privacy and the Group Manual Privacy from 2022 are less specific in this respect, as they mention that the DPO should be 'independent', but fail to specify that the DPO may only perform other tasks and duties if they do not result in a conflict of interests.[158]

In any event, a reference to the independence of the DPO in internal guidelines is not sufficient in itself to ensure compliance with Article 38(3) and (6) GDPR. To verify whether the controller has taken adequate measures to ensure that the DPO performs their tasks in an independent manner and that any additional tasks and duties do not result in a conflict of interests, other elements need to be considered too. In particular, it should be considered whether there are elements that may weaken the position of the DPO, and whether the other tasks that the DPO is asked to perform entail the advancement of interests that may conflict with data protection considerations.

While it is not uncommon for part-time DPOs to be a member of the legal team of their organisation, the duties normally assigned to a legal team also comprise tasks that may give rise to a conflict of interests for the DPO.[159] Therefore, when the DPO is a member of the legal team, it is of paramount importance to ensure that the DPO is only given other tasks or duties that are compatible with their role as DPO, and that it is clear – both to the DPO and the rest of the organisation – which tasks are performed in the capacity of DPO and which tasks are performed as a member of the legal team. In this respect, the Article 29 Working Party/EDPB has stated that an important element to avoid conflicts of interests is to ensure that 'the position of DPO or the service contract is sufficiently precise and detailed'.[160] The European Data Protection Supervisor (EDPS) has stated that:

> 'If the DPO is also a member of the legal team, organisational measures should be put in place to allow the DPO and their staff to clearly distinguish their activities, e.g. by having a separate functional mailbox for DPO matters (so that the rest of the

[157] 'Group Manual Privacy, Valid from: 01.06.2020', section 1.2.2.
[158] Group Manual Privacy, Valid from: 2022-01-01, section 1.1; Group Policy Privacy, Valid from: 2022-01-01, section 2.1.
[159] For example, a conflict of interests may arise if a DPO is asked to represent the controller in court in matters relating to the protection of personal data; see WP 243 rev.01 Guidelines on Data Protection Officers, adopted on 13 December 2016, approved by the EDPB in Endorsement 1/2018 of 25 May 2018, p. 17.
[160] Ibid.

> organisation can see whether the advice comes from the DPO function or legal advisory function).'[161]

In our view, the organisational measures put in place by Telenor ASA fail to ensure a clear distinction between the tasks performed as DPO and those that are to be performed as an Associate Lawyer.

Telenor ASA's functional job description for the employee to be hired as 'DPO & Associate Lawyer' describes the 'responsibility' of the employee as follows:

> 'Implement and/or develop as necessary policies, manuals, best practices, provide legal advice, and liase [sic] with external legal counsel. This shall be done in line with the risks and tasks identified by the Heads of Legal for Telenor Digital/Nordic Content/Technologies & Services/Telenor Norway and the prioritizations set by Head of Group Legal and Team Leader for Contracts & Content Team.
>
> - Inform and provide legal advice in alignment with other attorneys in Group Legal to Telenor ASA and the employees on their obligations pursuant to Data Protection Laws, regulations and other requirements.
> - Provide advice as regards the data protection impact assessment;
> - Cooperate with the supervisory authority;
> - Act as the contact point for the data protection supervisory authority on issues relating to processing, and to consult, where appropriate, with regard to any other matter.
> - On behalf of Telenor ASA seek prior consultation, where required, for high risk processing in absence of sufficient measures to mitigate such risk
> - As DPO for Telenor ASA report directly to the highest management level of the Telenor ASA on the status of data protection and urgent matters'.[162]

Furthermore, the tasks of the employee in question are described in the functional job description as follows:

> 'Implement and/or develop as necessary policies, manuals, best practices, provide legal advice (including contribute in relation to Authority Requests) and provide support during negotiations of contracts and liase [sic] with external legal counsel. Cooperate closely with other experts in Group Legal and other Group functions as required to support high risk or critical processes. Share information and best practice with colleagues in Group Legal.
>
> Act as DPO in accordance with the GDPR which entail the following activities as examples:
> - Develop and maintain Privacy Management Tools and Data Transfer Mechanisms
> - Contribute to Training and Awareness Program

[161] EDPS, Position paper on the role of Data Protection Officers of the EU institutions and bodies (30 September 2018), p. 11.
[162] DPO - Functional Job Description - Group Legal - Associate Lawyer & DPO – Excel.

- Contribute to embed Data Privacy Into Operations
- Inform and Advise on Data Protection Impact Assessments
- Inform and Advise on Integrating Privacy by Design into Data Processing Operations
- Contribute to management of Third-Party Privacy Risks
- Contribute to Privacy Notices
- Inform and Advise on Requests and Complaints from Data Subjects
- Monitor for New Operational Practices
- Develop and Evolve the Relevant Guidelines and Templates to Support Telenor ASA in Matters Regarding Protection of Personal Data
- Liaise with Group Compliance on related compliance activities'. [163]

In our view, even though there is an empty line in the Excel sheet separating the two paragraphs, this is not sufficient to clearly distinguish between the activities to be carried out as a DPO and those to be carried out as an Associate Lawyer. However, following our inspection, Telenor ASA argued that only the tasks expressly listed in the functional job description as examples of DPO activities are those to be fulfilled as a DPO, whereas the other tasks should be fulfilled as an Associate Lawyer. This ex-post statement with the aim of clarifying the relevant division of tasks fails to overcome the ambiguity of the functional job description. For example, Telenor ASA claims that it is exclusively in the capacity of Associate Lawyer that the employee should:

> 'Implement and/or develop as necessary policies, manuals, best practices […] in line with the risks and tasks identified by the Heads of Legal for Telenor Digital/Nordic Content/Technologies & Services/Telenor Norway and the prioritizations set by Head of Group Legal and Team Leader for Contracts & Content Team.'[164]

This is despite the fact that one of the examples of DPO activities in the functional job description is specifically to 'Develop and Evolve the Relevant Guidelines and Templates to Support Telenor ASA in Matters Regarding Protection of Personal Data'. Similarly, Telenor ASA claims that it is in the capacity of Associate Lawyer that the employee should 'Inform and provide legal advice in alignment with other attorneys in Group Legal to Telenor ASA and the employees on their obligations pursuant to Data Protection Laws, regulations and other requirements',[165] although that wording essentially mirrors the wording of Article 39(1)(a) GDPR concerning the tasks of the DPO.[166] The latter element is particularly concerning, as it suggests that the DPO's advice on data protection matters must be 'in alignment with other attorneys in Group Legal', which contradicts the requirement that the DPO should act independently.

We emphasise that working as a lawyer per se does not preclude the possibility of performing DPO duties, for example if the legal advice concerns areas of law other than data protection

[163] DPO - Functional Job Description - Group Legal - Associate Lawyer & DPO – Excel.
[164] DPO - Functional Job Description - Group Legal - Associate Lawyer & DPO – Excel.
[165] DPO - Functional Job Description - Group Legal - Associate Lawyer & DPO – Excel.
[166] Article 39(1) GDPR reads as follows: 'to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions'.

matters in the company.[167] This would be a matter to be determined on a case-by-case basis,[168] and the framework must be clear and concise.

Telenor ASA highlights the CJEU's decision in case C-453*/21 X-FAB Dresden*, which states, inter alia, that:

> 'a "conflict of interests", as provided for in that provision, *may* exist where a DPO is entrusted with other tasks or duties, *which would result in him or her determining the objectives and methods of processing personal data* on the part of the controller or its processor, which is a matter for the national court to determine, *case by case, on the basis of an assessment of all the relevant circumstances,* in particular the organisational structure of the controller or its processor and in the light of all the applicable rules, *including any policies of the controller or its processor*' (our italics).[169]

In our view, CJEU provides *examples* in this decision of circumstances that may suggest that the DPO has a conflict of interest. What is important here is that it is based on a case-by-case assessment of what constitutes a conflict of interest and whether the DPO is considered independent. Furthermore, we emphasise that the CJEU points specifically to internal guidelines in this assessment, which in this case are inadequate.

The Court's opinion referred to by Telenor ASA must also be read in the context of paragraph 40 of the same judgment:

> 'It thus follows from the wording of that provision, first, that the GDPR does not establish that there is a fundamental incompatibility between, on the one hand, the performance of DPO's duties and, on the other hand, the performance *of other duties* within the controller or processor. Article 38(6) of that regulation specifically provides that the DPO may be entrusted with performing *tasks and duties other than* those for which it is responsible under Article 39 of the GDPR.' (our italics)

The Court points out here that the DPO may perform other tasks and duties than those for which the DPO responsible pursuant to Article 39. Furthermore, 'the DPO cannot be entrusted with performing tasks or duties which could impair the execution of the functions performed by the DPO'.[170]

There must therefore be a clear distinction between tasks that the DPO performs by virtue of their role as DPO and other tasks. Such a distinction will be unclear or impossible if the DPO

---

[167] The assessment will differ for an internal lawyer and for an external lawyer who is hired as a DPO. For an external lawyer, there may be a clearer distinction between the individual clients and tasks (although here, too, there may be ties that challenge independence), while for an internal lawyer who provides advice on data protection matters in the company, it may be more difficult to maintain a clear distinction between the advisory function and, subsequently, the more objective role of DPO, where the interests of the data subjects are to be emphasised over the interests of the company.
[168] CJEU case C-453*/21 X-FAB Dresden v FC*, paragraph 46.
[169] Ibid. In the response, Telenor has cited the English language version of the judgment, as recited here.
[170] CJEU case C-453*/21 X-FAB Dresden v FC,* paragraph 41.

performs similar tasks or tasks that a DPO is set to oversee. In this context, we refer to the description of tasks and duties reproduced above, which shows tasks that are largely practical data protection tasks and for which the DPO has an advisory or control function.

The lack of clarity with respect to the activities that are carried out as DPO and those that are carried out as an Associate Lawyer is exacerbated by the fact that there is no evidence to suggest, in the timeframe of the inspection, that Telenor ASA's DPO used a separate mailbox for DPO matters.[171] Furthermore, the current DPO's email signature mentions both of her roles as follows:

> **N.N.**
> Associate Lawyer and Data Protection Officer (DPO) Telenor ASA
> Group Legal
>
> Telenor Group
> +47 xxxxxxxx
> Snarøyveien 30
> N-1360 Fornebu
> www.telenor.com
>
> Facebook | Twitter |LinkedIn
>
> 

Thus, a colleague who receives an email with data protection advice from her would be unable to distinguish whether the advice comes from the DPO function or the legal advisory function.

Under Norwegian law, the supervisor ('prinsipal') of a associate lawyer ('advokatfullmektig') has a duty to provide guidance to the associate lawyer,[172] and the trainee lawyer has a duty to keep the supervisor informed about the work performed.[173]

In its comments on the notification, Telenor ASA states that:

> 'The supervisor-trainee lawyer relationship does not apply to the role of DPO. The point of view therefore assumes that the supervisor as a lawyer will act contrary to the requirement for independence. This is a purely theoretical risk and it applies to all

[171] We note the email address 'tnasa_dpo@telenor.com' in Telenor ASA's privacy policy updated on 3 February 2022, but Telenor ASA has not supplied us with any evidence to suggest that that email address either existed or was used in the timeframe of the inspection.
[172] Regulations for the Courts of Justice Act (Regulations for Advocates) Re Chapter 12 ('Til kapittel 12 Regler for god advokatskikk i advokatforskriften'), sections 5.6 and 5.7.
[173] See the Norwegian Bar Association ('Advokatforeningen, Veiledning for prinsipal og advokatfullmektig' (22 November 2019)).

> superior and subordinate relationships, not just the supervisor-trainee lawyer relationship. On the other hand, it must be assumed that a superior who is a lawyer has a particular awareness of roles and independence, and that the risk of independence being compromised is therefore lower than would otherwise be the case.'

We note that the head of a legal team is normally the one who decides (at least in part) on the purposes of the personal data processing carried out by the team in connection with the performance of the tasks assigned to the team (e.g. which personal data are to be processed in connection with legal processes). It is possible that the supervisor-trainee lawyer relationship will affect the proper performance of DPO tasks with respect to processing activities carried out or otherwise affected by the work of the supervisor, as a trainee lawyer may have difficulties standing up to their supervisor. Although the supervisor-trainee lawyer relationship only applies to the associate lawyer role, we believe there is a risk that the person in question may be more concerned with acquiring a licence as a lawyer than with the performance of their tasks and duties as a DPO. All risks, including theoretical ones, must be specifically assessed to determine the DPO's independence and whether a conflict of interest exists. These assessments should be documented as part of the internal control referred to in Article 24(1) GDPR.

The proper performance of DPO tasks often requires the DPO to take a firm and insisting attitude, also vis-à-vis employees who hold a superior position and have decision-making power within the organisation, which may be perceived, at best, as bureaucratic or, at worst, as unpleasant 'trouble-making'. Thus, the DPO must be in a position to withstand the pressures and difficulties that accompany this important position.[174]

The fact that, in Telenor ASA, the budget for data protection-related expenses is 'allocated on a case-by-case basis by line management'[175] further weakens the DPO's position. A DPO who must request resources from their direct superior could face difficulties, in particular if the latter is not fully committed to achieving data protection compliance.[176] In the present case, Telenor ASA's DPO does not have their own budget line and needs to seek the budget for data protection expenses from their line manager, who is also one of the DPO's supervisors ('prinsipal'). This may have negative consequences for the independence of the DPO.

Finally, during the course of the inspection it became apparent that all DPOs in the Telenor Group, including the DPO of Telenor ASA, own shares in the company.[177] Telenor ASA has neither assessed whether this may generate a conflict of interests for the DPOs nor drawn up internal rules to prevent possible conflicts of interests for DPOs in their capacity as shareholders. It is a well-known issue that, for some professions that require a high degree of

---

[174] See Network of Data Protection Officers of the EU Institutions and Bodies, Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (14 October 2010), p. 6.
[175] 'Response to Datatilsynet additional documentation', 10 January 2022, p. 4.
[176] See Network of Data Protection Officers of the EU Institutions and Bodies, Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (14 October 2010), p. 6.
[177] Final inspection report of 30 September 2022, p. 25.

independence (e.g., lawyers), ownership of shares in a company may be incompatible with the requirement for independence. In particular, this may be the case if the shareholder who is subject to such a requirement performs activities that may have an impact on the value of the shares.[178] This is the case with respect to many activities of a DPO whose advice, if followed, may lead to substantial changes to the company's business model. Thus, owning shares in the company may generate a conflict of interests for a DPO who is also a shareholder, in particular if there are no limits on the amount of shares they may acquire. In turn, this may affect the independence of the DPO when the latter is asked to advise on particularly business-critical processing operations. As Telenor ASA points out in its response, we are talking about a low number of shares in this case. It is not automatically the case that share ownership leads to a conflict of interest, but it is an issue that Telenor ASA should have considered and documented.

We have not considered the external DPO's independence or possible conflicts of interest, but note that he was hired as an external consultant for a limited period of time. At the time of the inspection, his degree of independence was thus structurally different from the DPO, who was permanently employed in the position of both DPO and Associate Lawyer.

We also note that, during the six-month timeframe of the inspection when the DPO held two roles, she essentially worked full-time on DPO tasks, insofar as the DPO tasks were distinguishable from the associate lawyer tasks (which Datatilsynet does not believe they always were). Thus, there was a lower risk of conflicts of interest materialising in practise. However, some of the circumstances discussed above nevertheless challenge the DPO's independence, for example in relation to the dependency relationship for acquiring test cases and a licence as a lawyer. Such dependency can under certain circumstances have unfortunate consequences, for example if a DPO chooses to prioritize down getting involved in demanding cases that make the concerned DPO seem as a 'trouble-maker', for the sake of further career development. Datatilsynet has doubts as to whether the role of in-house Associate Lawyer can at all be combined with the DPO role.

Datatilsynet does not have enough information to conclude on this point. Regardless, we do find that Telenor ASA has not carried out all the assessments it should have and that the distinction between the roles and tasks of DPO and Associate Lawyer, respectively, was not sufficiently clear. See section 12.2 on the requirements of Article 24(1) and (2) GDPR.

11 Tasks of the DPO – Article 39(1)

11.1 Inspection criteria and evidence

The first and second sentences of Article 39 GDPR read as follows:

1. The data protection officer shall have at least the following tasks:

[178] See https://www.advokatforeningen.no/advokatetikk/regler-og-retningslinjer/uttalelser-fra-etikkutvalget/10-betaling-for-advokatbistand-med-aksjer/

a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
d) to cooperate with the supervisory authority;
e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

We further refer to sections 3.8.1 and 3.8.2 in the final inspection report of 30 September 2022.

11.2 **Datatilsynet's assessment**

Overall, the tasks set out in Article 39(1) are reflected in the job description of Telenor ASA's DPO, the Group Manual Privacy from 2020[179] and the Group Manual Privacy from 2022.[180] Even though we are of the opinion that the description of the DPO's tasks should be more specific, for example with regard to how and when the DPO should be involved in the handling of personal data breaches and DPIAs, we do not conclude that Article 39(1) GDPR has been violated within the timeframe of the inspection, as the preponderance of evidence is insufficient.

12 Organisational measures to ensure compliance – Article 24(1) and (2)

12.1 **Inspection criteria and evidence**

Article 24(1) and (2) GDPR reads as follows:

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is

[179] 'Group Manual Privacy, Valid from: 1 June 2020', section 2.2.2.
[180] 'Group Manual Privacy, Valid from: 1 June 2020', section 1.1.

performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

We refer to sections 3.9.1 and 3.9.2 in the final inspection report of 30 September 2022.

12.2 **Datatilsynet's assessment**

Article 24(1) states that the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is compliant with GDPR. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

12.2.1 **Scope of controllership**

The processing operations carried out by Telenor ASA encompass different categories of personal data.[181] From Telenor ASA's Article 30 report, it seems that a limited amount of personal data processed by Telenor ASA falls within the definition of special categories of personal data, cf. Article 9(1) GDPR.[182] Telenor ASA mostly processes personal data relating to its own approximately 380 employees, but also about other employees of the Telenor Group (about 15,000 in total[183]), as well as customers and other individuals.[184] Even though Telenor ASA does not have direct customer relations, it processes customer data originally collected by its subsidiaries within Group-Unit-Internal Audit & Investigations (GIAI) and Telenor Research.[185] Telenor ASA also processes data that originally stem from the subsidiaries in the day-to-day monitoring of their compliance with group policies in the Compliance department.[186]

Processing activities carried out by Telenor ASA's subsidiaries are only relevant for the present case to the extent Telenor ASA qualifies as controller, alone or jointly with the relevant subsidiary, or where Telenor ASA qualifies as processor and/or the relevant subsidiary acts as processor or sub-processor for Telenor ASA.

It is beyond the scope of the present inspection to conclude on Telenor ASA's role in all the different processing activities that are carried out by the company and its subsidiaries. However, taken together, the relevant facts in the case can say something about the obligations incumbent on Telenor ASA.

---

[181] Final inspection report of 30 September 2022, pp. 4–5.
[182] Telenor ASA's Article 30 record of 2 February 2022.
[183] Final inspection report of 30 September 2022, p. 10.
[184] Telenor ASA's Article 30 record of 2 February 2022.
[185] Final inspection report of 30 September 2022, pp. 4–5.
[186] Final inspection report of 30 September 2022, pp. 4–7 and 10.

Which role Telenor ASA has regarding the different processing activities has consequences for the company's responsibilities. For instance, a processor must only process data on documented instructions from the controller pursuant to Article 28(3)(a) GDPR. A controller, on the other hand, is responsible for and must be able to demonstrate compliance with the principles relating to the processing of personal data pursuant to Article 5(2) GDPR. Furthermore, as mentioned, Article 24 GDPR is aimed at the controller.

In relation to its subsidiaries, Telenor ASA acts as controller, joint controller and processor.[187] Telenor ASA's role must be considered individually in each situation. Controllership rests with the company or companies that, alone or jointly with others, determine the purposes and means of the processing of personal data, cf. Article 4(7) GDPR. One of the main elements in this regard is who exerts decisive influence over the processing for their own purposes.[188] For instance, a controller may exert influence over the processing of personal data for the purpose of fulfilling legal obligations.[189] When a company in the Telenor Group processes personal data on behalf of the controller, it qualifies as processor pursuant to Article 4(8) GDPR.

Telenor ASA maintains that the other companies in the Telenor Group act as separate controllers for their own processing activities, and for processing activities that Telenor ASA conducts involving data originally collected by the other companies.[190] Especially relating to the processing of customer data, Telenor ASA maintains that they act as processor on behalf of its subsidiaries.[191] However, according to the Article 30 report, Telenor ASA qualifies as controller, e.g. for the processing of personal data about employees in the Telenor Group for 'Corporate Social Networking' and 'Learning Management Systems.' It is in any case the actual circumstances that are decisive for the assessment of who the controller is.[192] If Telenor ASA in a specific context exerts influence over the processing to the degree that it (co-) determines the purposes and means of the processing of personal data by its subsidiaries, Telenor ASA will be (joint) controller for that processing.

The CJEU has ruled that the term 'controller' must be broadly defined and that:

> 'the existence of joint responsibility does not necessarily imply equal responsibility of the various operators engaged in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case.'[193]

---

[187] Final inspection report of 30 September 2022, p. 6.
[188] CJEU Case C-25/17, *Jehovah's witnesses*, ECLI:EU:C:2018:551, paragraph 68.
[189] EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 2.0 (adopted on 7 July 2021) p. 13.
[190] Final inspection report of 30 September 2022, pp. 3–8 and 10.
[191] Final inspection report of 30 September 2022, pp. 3–4, 5 and 8.
[192] EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, p. 13.
[193] CJEU Case C-25/17, *Jehovah's witnesses*, ECLI:EU:C:2018:551, paragraph 66. See also Case C-210/16 *Wirtschaftsakademie* EU:C:2018:388, paragraphs 28, 43 and 44.

Furthermore, the joint responsibility of several actors 'does not require each of them to have access to the personal data concerned'.[194]

Telenor ASA processes customer data e.g. for the purposes of research through surveys in the Telenor Group's markets to understand customer behaviours.[195] These are multi-country, multi-year surveys, with business and research purposes.[196] Telenor ASA defines itself as processor for this specific processing.[197] The fact that these investigations are carried out on a large scale throughout the Telenor Group, and that they encompass the different markets of the Telenor Group and with a purpose of understanding customer behaviours in these markets, suggests that it is not only the subsidiaries of Telenor ASA that qualify as controllers for this processing. It seems unlikely that Telenor ASA does not, at least to some degree, exert influence over the purposes and means of this processing. Datatilsynet is of the opinion that this could be a processing activity for which Telenor ASA may have joint controllership with its subsidiaries.

Furthermore, there are several situations in which the subsidiaries are given responsibility for how to implement instructions, e.g. through the group's governing documents.[198] In some cases, these documents define the framework for the subsidiaries' activities, including with regard to the processing of personal data. In light of this, Datatilsynet is of the opinion that Telenor ASA acts as joint controller together with its subsidiaries for some of the processing activities carried out in the Telenor Group. However, we do not conclude on this point, as this must be considered by Telenor ASA.

The external DPO described the situation as follows:

> '[…] as long as ASA has an operational involvement in business activities involving processing of personal data, whether it's within ASA itself or exercised upon other businesses through ASAs role as HQ, there are privacy obligations to adhere to that ASA cannot fully escape.'[199]

As mentioned previously, it falls outside the scope of the present inspection to reach a firm conclusion on Telenor ASA's role in the different processing activities in the Telenor Group. Such clarification will be a task in which a DPO, with their data protection expertise and knowledge of the company, should be involved.

In this case, we only rely on what Telenor ASA has written in their own the records of processing, to the extent that there is only a requirement of preponderance of evidence.

---

[194] CJEU Case C-25/17, Jehovah's witnesses, ECLI:EU:C:2018:551, paragraph 69 and Case C-210/16 *Wirtschaftsakademie* EU:C:2018:388, paragraph 38.
[195] Final inspection report of 30 September 2022, p. 5.
[196] Telenor ASA's Article 30 record of 2 February 2022.
[197] Telenor ASA's Article 30 record of 2 February 2022.
[198] Final inspection report of 30 September 2022, p. 6.
[199] Final inspection report of 30 September 2022, p. 9.

Based on the evidence obtained from the inspections, we find it unclear in several cases whether Telenor ASA should be considered controller, joint controller or processor for specific processing activities. That is the case for processing both by other companies in the Telenor Group and by Telenor ASA relating to data originally collected by other companies of the group. However, we find it to have been substantiated that Telenor ASA acts as controller for more activities than the company has assumed in its responses to Datatilsynet.

12.2.2 **Regarding organisational measures**

In this section we assess the organisational measures that Telenor ASA had in relation to Article 38 GDPR and for general compliance of the GDPR.

In accordance with the accountability principle in Article 5(2) GDPR, Telenor ASA shall be responsible for, and be able to demonstrate compliance with, the other principles of data processing.

It follows from Article 24(1) GDPR that the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is compliant with the GDPR.

Article 24(2) states that, where proportionate in relation to the processing activities, the controller shall implement appropriate data protection policies. This entails that the organisational measures should include internal data protection policies where relevant and proportionate.

Telenor ASA is, in any case, controller for a number of processing activities regarding employee data. For these type of processing activities, which take place in a professionalised context and in the context of a large group, it is clearly reasonable to expect at least fundamental guidelines and a minimum level of internal control to ensure GDPR compliance. Anything else would undermine the purpose of Article 24 and the accountability principle.

We note that further processing activities for which Telenor ASA is identified as the controller alone or jointly may impose even stricter requirements regarding which policies must be in place.

For the sake of completeness, we emphasise that organisational measures, documentation and policies must specify *how* the company should achieve GDPR compliance. It is, of course, not sufficient to simply repeat or refer to the wording of the GDPR.

Telenor ASA must therefore adopt a written policy, with clear and precise content, as outlined below. The documented policy should provide detailed descriptions that the Telenor ASA can refer to and use internally with respect to organisation of the DPO within the company.

In its response, Telenor ASA indicated that what is decisive is whether the measures have an effect.[200] It is in any case Telenor ASA's responsibility to ensure that the policy is formalised and documented so that compliance can be demonstrated, and to prepare the policy in such a way that it is possible to operationalise the guidelines and enable them to have an effect.

Firstly, we refer to section 6.2 above, where we concluded there was a risk that Telenor ASA's DPO was not being involved in all data protection issues in a proper and timely manner. We were not presented with any policy that demonstrated or ensured the involvement of the DPO. For this reason, it has been difficult to determine whether or not the requirement in Article 38(1) GDPR was met. We have given the company the benefit of the doubt.

Telenor ASA considers that there are no grounds for requiring a formalised policy since we chose not to conclude that Article 38(1) GDPR had been violated.[201] The fact that the absence of a policy has made it difficult for Datatilsynet to conclude on these questions cannot be understood to mean that no violation has taken place. We consider that the lack of a policy constitutes an independent violation of Article 24 GDPR and believe there is a need for documented assessments as part of the internal control.

Datatilsynet finds the degree of formalisation of the *timing* and *manner* of involvement of the DPO insufficient. Telenor ASA has not provided us with any written procedures or other appropriate policies regarding the timing and manner for involvement of Telenor ASA's DPO in all data protection issues, including DPIAs and data breach management. The inspection has revealed that the involvement of the DPO in data protection matters has generally been informal and to a large extent been decided on a case-by-case basis. We therefore find Telenor ASA failed to establish organisational measures to ensure and demonstrate that all processing activities were performed in accordance with the GDPR, and had not implemented sufficient internal policies regarding when and how to involve the DPO in all data protection issues.

Secondly, we refer to section 8.2 above, where it is our view that Telenor ASA has failed to demonstrate the existence of organisational measures in the form of a formalised reporting line between the DPO and the highest level of management[202] of Telenor ASA, within the timeframe of the inspection. The issue was raised by the external DPO.[203] Telenor ASA has not provided us with any formally adopted written policy describing or ensuring the DPO's access to the highest management level. As the discussion in section 8.2 shows, it is essential that the company considers how and to whom the reporting should take place in practise and concretizes this in clear and unambiguous written guidelines. This has lacked in Telenor ASA.

[200] Ibid.
[201] Comments on the advance notification of 31 May 2024, pp. 47–48.
[202] Cf. Article 5(2) and Article 24 GDPR.
[203] 2021.09.09 – TNASA Privacy status and proposals for GU Forum, p. 13, Section 8.2, pp. 32–33.

We specify that mentioning the DPO's possibility of reporting directly to the 'CEO first escalation' and the 'BoD second escalation' (board of directors)[204] in PowerPoint presentations is not sufficient in this case.

We note that the new and updated policies, Group Manual Privacy and Group Policy Privacy, valid from 1 January 2022, still do not mention the reporting line to the board. The following sentence from the Group Manual Privacy (valid between 1 June and 31 December 2021) was even removed in the updated version that entered into force on 1 January 2022:

> 'The DPO shall have the right to report all privacy-related incidents and non-conformities directly to the BU CEO.'[205]

In this case, we have seen different interpretations in Telenor ASA's documentation of what should be considered the highest management level. We are of the opinion that internal policies for the company must clearly define the highest management level in Telenor ASA and provide a description of how the DPO is ensured a direct reporting line accordingly.

In essence, Telenor ASA's decisions on using CCM and GU Forum as reporting arenas and the mentioned amendments to its former manuals and policies demonstrate how unclear the content in the internal policies has been. Even though it would be possible for a DPO to reach out informally to the board and day-to-day highest management, this would most likely be dependent on personal acquaintances and perhaps by chance of circumstances. Either way, companies must have appropriate organisational measures in place, including internal policies that are reliable and available in all circumstances to be able to ensure and demonstrate compliance,

Thirdly, we refer to section 10.2 above. where Datatilsynet did not have enough information to conclude if the DPO was ensured sufficient independence and absence of conflict of interests. A concrete and documented analysis of possible risks should have been conducted in this respect. As previously mentioned, we find that the organisational measures put in place by Telenor ASA failed to ensure a clear distinction between the tasks to be performed as DPO and those to be performed as Associate Lawyer. There are several organisational measures that would have been appropriate, ranging from placement in the organisation to avoid dependencies, to the DPO needing to use a separate email address to clearly show the distinction between roles. In addition, Telenor ASA has neither assessed whether the fact that DPO owns shares in the company may generate a conflict of interests for the DPO nor implemented organisational measures to prevent possible conflicts of interests for DPOs/shareholders. We consider Telenor ASA's implementation of organisational measures to be inadequate in this regard. We find that these efforts do not fulfil the legal requirements of Article 24(1) GDPR. In any case, Telenor ASA is not able to demonstrate compliance with the provisions of the GDPR.

---

[204] TNASA Privacy organisation overview, per 2021.12.06 and 2021.09.09 – TNASA Privacy status and proposals for GU Forum.pdf

[205] Group Manual Privacy, valid from 1 June 2020, p. 5.

Fourthly, we refer to our assessment in section 8.2, where we quote directly from the former Group Manual Privacy policy, which stated that 'GPO shall act as DPO in Telenor ASA'.[206] Telenor ASA noted in its comments on the inspection report that 'DPO' in this respect is meant to refer to the fact that, at the time, the DPO was organisationally placed in the division Group Privacy & IM and not Group Legal.[207] Telenor ASA also claims that the DPO's responsibility and tasks are not presented in the Group Manual Privacy since it relates to Telenor as a group.[208] Telenor ASA emphasised that the GPO and DPO have always been two separate roles.[209] Datatilsynet notes that Telenor ASA has kept us up to date regarding who has the role of DPO in Telenor ASA, and that [redacted] was the GPO when someone else had the role of DPO. This shows that Telenor ASA's practice differed from what was written in the internal group policy. Telenor has acknowledged that 'they understand that the text is imprecise and can be misunderstood'.[210] It is difficult to see why it is stated in the policy that the GPO shall act as DPO in Telenor ASA when that is not the case.

In its comments on the notification, Telenor ASA states that:

> 'It has not been elaborated or stated what measures Datatilsynet considers necessary on the basis of the Group Privacy Manual. To the extent that Datatilsynet considers that the wording of this policy needs to be adjusted, Telenor will again emphasise that the matter does not constitute an independent violation of Article 24(1) and (2) GDPR. Such a change will not have an actual effect as regards the DPO's position in Telenor ASA.'

Furthermore, Telenor ASA questions whether Article 24(1) and (2) GDPR on an independent basis provide for special guidelines on DPOs. Telenor ASA asserts that 'the internal control provision in Article 24(1) and (2) GDPR targets the "processing" and is intended to ensure that the processing of personal data is in accordance with the requirements of the GDPR'.[211] Their interpretation is thus that Article 24 GDPR only applies to the individual processing activity, and not in general. However, this is a narrow understanding of the provision with which we do not agree.

It follows from several sources of law that Article 24 GDPR is an internal control provision, as Telenor ASA also states, and that it applies to GDPR compliance in general. Recital 78 states it is required 'that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met.' In other words, the purpose and the legislator's intention, is that the requirement for appropriate technical and organisational measures to ensure compliance, applies generally and not only for the 'processing.'

Both Jarbekk et al. and Skullerud et al. refer to Article 24 GDPR as internal control and that the provision is very much a continuation of the internal control provision in the former

---

[206] 'Group Manual Privacy, valid from: 2020-06-01', pp. 3–4.
[207] 'Preliminary inspection report – With comments from Telenor ASA in yellow', 16 May 2022, p. 12.
[208] 'Preliminary inspection report – With comments from Telenor ASA in yellow', 16 May 2022, p. 12.
[209] 'Preliminary inspection report – With comments from Telenor ASA in yellow', 16 May 2022, p. 12.
[210] 'Preliminary inspection report – With comments from Telenor ASA in yellow', 16 May 2022, p. 12.
[211] Comments on the advance notification of 31 May 2024, p. 49.

Personal Data Act (2000) Section 14.[212] Jarbekk et al. state that 'the controller shall implement 'appropriate technical and organisational measures' to 'ensure and demonstrate' compliance with the regulation' (our emphasis).[213]

In other words, it is a provision that establishes what is fairly obvious, namely that the controller has a duty to comply with all relevant provisions of the GDPR. Article 24 GDPR must be interpreted in light of Article 5(2) GDPR and the accountability principle, and must be read as a provision on 'accountability.'[214] The provision was introduced because the previous Data Protection Directive's system of providing notification to the data protection authorities was discontinued.[215] This means that responsibility for compliance rests fully with the controller.[216]

It would be directly contrary to the purpose and context of the provision, cf. the EEA law interpretation principles mentioned above, if the controller only needed to ensure compliance with certain provisions of the GDPR. In practice, this would have entailed that the controller did not need to ensure compliance with the other provisions. It is clear for Datatilsynet that the legislator has not made such a rule.

As Docksey points out, Article 24 GDPR has evolved from the Data Protection Directive in that it requires proactive and demonstrable compliance:

> 'It places responsibility firmly on the controller to take proactive action to ensure compliance and to be ready to demonstrate that compliance. (…) Accountability in this sense requires that controllers put in place internal policies and mechanisms to ensure compliance and provide evidence to demonstrate compliance to external stakeholders, including supervisory authorities.'[217]

> 'It is crucial for controllers to take active responsibility for ensuring compliance and develop an accountability culture at all levels of their organisation.'[218]

The obligation to provide documentation follows from Article 24(2) GDPR. As Skullerud et al. point out:[219]

---

[212] Eva Jarbekk et al.: *Personopplysningsloven og personvernforordningen med kommentarer* (2019), p. 256. Åste Marie Bergseng Skullerud, Cecilie Rønnevik, Jørgen Skorstad and Marius Engh Pellerud: *Personopplysningsloven og personvernforordningen (GDPR), kommentarutgave* (2019), p. 273.
[213] Eva Jarbekk et al.: *Personopplysningsloven og personvernforordningen med kommentarer* (2019), p. 256.
[214] Christopher Docksey, 'Article 24 Responsibility of the controller' in Kuner, Bygrave and Docksey (eds.), *The EU General Data Protection Regulation (GDPR). A commentary*, p. 557
[215] Christopher Docksey, 'Article 24 Responsibility of the controller' in Kuner, Bygrave and Docksey (eds.), *The EU General Data Protection Regulation (GDPR). A commentary*, p. 560
[216] Ibid.
[217] Christopher Docksey, 'Article 24 Responsibility of the controller' in Kuner, Bygrave and Docksey (eds.), *The EU General Data Protection Regulation (GDPR). A Commentary,* pp. 555–570.
[218] Ibid p. 568
[219] Åste Marie Bergseng Skullerud, Cecilie Rønnevik, Jørgen Skorstad and Marius Engh Pellerud: *Personopplysningsloven og personvernforordningen (GDPR), kommentarutgave* (2023), online comments on Article 24.

> ‘The company’s internal procedures must be established and documented in writing.’
>
> ‘As part of the internal control system, the controller shall implement governing documents addressing data protection for data subjects, cf. Article 24(2) GDPR. According to the Personal Data Act (2000), it was also considered a requirement to establish governing documents for the undertaking’s processing of personal data.’

Datatilsynet therefore finds that the company’s narrow understanding of Article 24(1) GDPR must be rejected.

Furthermore, when a DPO has been appointed, it is a requirement that the DPO has independence, necessary resources, direct reporting line to highest management, and is involved in all data protection issues. As an example, if the requirements relating to independence are failed to be respected, it may result in the processing activities in which the DPO has been involved fail to comply with the GDPR. The same is the case if, for example, the DPO has not been involved in processing activities where the DPO’s involvement was required or if the DPO was unable to report any deficiencies to the highest management level. In other words, there is always a link – albeit indirectly – between specific processing and policies relating to the DPO. If the documentation relating to the DPO is inadequate, it will simply not be possible for the controller to demonstrate that the processing complies with the law, as required by the provision.

Article 24(1) GDPR states that the controller shall be able to demonstrate compliance. Incorrect and contradictory policies are obviously not in line with this requirement. Failure to demonstrate compliance is thus a violation in itself, regardless of whether an actual effect can be established; the point is precisely that, when the documentation is inadequate, it will often not be possible for the supervisory authority to uncover the facts.

In its response, Telenor ASA indicated that Article 24 requires a proportionality assessment:

> ‘Telenor cannot see that Article 24 GDPR necessitates guidelines to the extent and level of detail Datatilsynet requires, when this is not related to the processing activities themselves, but rather to the DPO (who is not directly involved in the processing activities).’

As mentioned Datatilsynet has pointed out that Telenor ASA is lacking fundamental internal policies. To require the policies to be neither contradictory nor incorrect is hardly too much to ask. Already here, we believe that Datatilsynet’s requirements are within the scope of what can reasonably be expected from Telenor ASA.

Furthermore, the inspection has revealed some policies that are not concrete, and the data protection work has taken place in the context of several different forums. Based on the complexity, that has been uncovered through the inspection, on Telenor ASAs organisation of the data protection work and ambiguities around the scope of processing activities, it will be proportionate to implement concrete guidelines.

We consider that Telenor ASA's policies concerning the DPO were inadequate. In part, they simply repeated the wording of the law, in part they were self-contradictory, and in part they did not provide sufficiently detailed instructions for Telenor ASA's DPO arrangement. The findings and issues addressed in this decision are largely a consequence of these inadequate policies. No appropriate organisational measures had been established to ensure that the role was actually independent, that the DPO was involved in all issues relating to data protection and that they had access to the highest management level in line with the intention of the law.

Fifthly, we find that Telenor ASA lacks organisational measures to ensure general GDPR compliance.

[redacted] wrote in an email to [redacted] dated 12 April 2021:

> 'Regarding Data Protection/Transfer Impact Assessments, the current backlog is quite big and I believe the organization is struggling a bit to get up to speed. There is currently little capacity/competency to conduct proper impact assessments among the ASA colleagues.'[220]

The external DPO was copied in the above email and responded, among other things:

> 'True. However, the lack of capacity/competence to conduct assessments is also a symptom of a more general issue of immature privacy compliance governance and performance at ASA, and a lack of foundational building blocks for privacy compliance, such as e.g. inventory, awareness and competence, operational capacity, implemented processes and unclear roles/responsibilities for group initiatives'.[221]

In relation to a discussion on outsourcing of operational GDPR compliance activities, the external DPO wrote the following:

> 'However, more generally than simply discussing outsourcing of some operational privacy compliance activities (which also would have a time- (in terms of follow-up/involvement) and monetary cost to ASA), this discussion/issue between the mentioned entities foundationally has to do with defining each entity's role (privacy wise) and corresponding accountability, responsibilities and operational capacity in initiatives with group dependencies'.[222]

Telenor ASA has informed us that they did not go through with the outsourcing that was under discussion and that this is therefore irrelevant.[223] In our view, the above correspondence, regardless of whether the outsourcing happened or not, is relevant because it illustrates that, at the time when it was written, there was uncertainty in Telenor ASA regarding the allocation of data protection roles (i.e. when Telenor ASA acts as controller, joint controller or processor with or on behalf of other business units), the accountability and

[220] '2021.04.13 – Mail to EVP People'.
[221] '2021.04.13 – Mail to EVP People'.
[222] '2021.04.13 – Mail to EVP People'.
[223] Final inspection report of 30 September 2022, p. 30.

operative capacity.[224] We find inadequate implementation of appropriate organisational measures regarding these issues to ensure and demonstrate that processing is performed in accordance with the GDPR.

According to the external DPO, there was a general diffusion of responsibility[225] and a lack of competence in Telenor ASA.[226] Based on the evidence collected during the present inspection, we agree with this assessment. We refer to section 5.2.3 regarding our assessment of diffusion of responsibility and unclear allocation of roles in Telenor ASA.

Furthermore, we find the internal policies should have been better structured on several specific and general data protection issues, as the former DPO also pointed out.[227] At the meeting of the GU Forum in September 2021, the former DPO presented, among other things, the following regarding data protection and privacy governance in Telenor ASA:

> 'b) Routines, policies and documentation - The organization lacks structured and documented frameworks and ways-of-work to adhere to privacy requirements, causing inefficiencies, unclarity and direct non-compliance.
> c) Internal data sharing governance - Personal data is shared between business units within Telenor without adequate data sharing governance, including legal transfer mechanisms, clear definition of controller/processor relationships, and generally diffusion of responsibility.
> d) Business-, system- & contract ownership - Ambiguous/nonstandardized governance for internal business-, system- and contract ownership, as well as potential GSSoutsourcing/operation capacity, causing ambiguity and diffusion of responsibility for privacy compliance.
> e) Line org. capacity and competence - The organization lacks capacity and competence to deal adequately with privacy compliance pro-actively, causing strain on existing resource(s), process and progress bottlenecks, and ultimately low /noncompliance'.[228]

In addition, the external DPO noted the presence of risks in relation to the privacy principles, privacy notices, personal data breaches, DPIAs (Data Protection Impact Assessments), sharing of personal data with non-compliant third parties, and sharing of personal data with third parties without formal statutory requirements including international transfers.[229] When identifying these types of serious privacy risks, it is clear under Article 24(1) GDPR that the controller must address them. Telenor ASA has not done so.

We note that Telenor ASA has adopted internal privacy principles and policies[230] that they claim are reviewed and updated as required. A new Group Manual Privacy was shared with us

[224] Final inspection report of 30 September 2022, p. 30.
[225] See also section 5.2.3.
[226] '2021.04.13 – Mail to EVP People'
[227] '2021.09.09 – TNASA Privacy status and proposals for GU Forum.pdf'
[228] '2021.09.09 – TNASA Privacy status and proposals for GU Forum.pdf', p. 13.
[229] '2021.09.09 – TNASA Privacy status and proposals for GU Forum.pdf', pp. 15–20.
[230] 'Group Policy Privacy, valid from: 2022-01-01'

on 13 December 2021, to become valid from 1 January 2022, that included changes in the direction of better GDPR compliance. However, this is not sufficient, as during the timeframe of the inspection, there was a lack of organisational measures to address the issues mentioned above.

If this case had involved a small business with just a few employees, more informal policies would perhaps have been be sufficient, but this is not practical in a company with an extensive business area and many employees. In this context, we point out that Telenor ASA is the parent company of one of the largest Norwegian groups in the telecom sector. At the time of the inspection, Telenor ASA was responsible for adopting global policies, and we believe that it must be expected that the parent company that decides data protection policies is able to operationalise them through specific procedures and policies. The lack of specific policies is also in contrast to Telenor ASA's operations in other areas, which are governed by many corporate governance documents. As Telenor ASA also refers to in its response, they operate in a sector that is strictly regulated, with a strong emphasis on compliance. It is therefore natural to set similar requirements for compliance in the area of data protection as for other business-critical areas.

The external DPO described the risk of being unable to perform the role effectively and independently.[231] In our opinion, one of the reasons for this was the lack of proper implementation of clear policies, including a clear reporting line and access to the highest management and clear description of the DPO's tasks.

Overall, our assessment is that Telenor has violated Article 24(1) and (2) GDPR by not having implemented appropriate organisational, that ensure and demonstrate compliance and by not having had adequate policies in place.

13 Assessment of corrective measures

13.1 Summary of findings in relation to corrective measures

With reference to the assessments in section 5, we note that Telenor ASA has not carried out an internal and documented assessment of the obligation to appoint a DPO, which is a necessary part of internal control and thus constitutes a violation of Article 24 GDPR.

Furthermore, in section 5, we pointed out that Telenor ASA has admitted that the company did not have adequate routines in terms of completing and updating the record of processing activities. Telenor ASA notes the record of processing activities contains ambiguities.[232] As pointed out in section 5 the record of processing activities is a part of internal control, and

'Group Manual Privacy, valid from: 2022-01-01'
'Group Manual Privacy, valid from: 01.06.2020'
'2020 Mandate and Functional Description Group Privacy and IM (share)'
'Old Group Privacy IM mandate (pre 2021)' 1 March 2020.
[231] '2021.09.09 – TNASA Privacy status and proposals for GU Forum', p. 13.
[232] Comments on the advance notification of 31 May 2024, p. 11.

Article 24 GDPR requires organisational measures to ensure that the record is correct and updated at all times.

With reference to the assessments in section 8, we found that Telenor had not established a formalised and direct reporting line for the DPO to the highest management level for most of the timeframe of the inspection, in violation of Article 38(3) GDPR.

With reference to the assessments in section 12, we found that Telenor ASA has not implemented organisational measures to ensure compliance with the GDPR and has not demonstrated compliance, in violation of Article 24(1) GDPR, and has not implemented appropriate data protection policies, in violation of Article 24(2) GDPR, regarding organisational measures linked to Article 38 GDPR and general compliance with the GDPR.

Regarding the partial violation of Article 37(7) GDPR, we note this as a minor infringement for a limited amount of time, which has been corrected. Therefore, we consider that no further action or corrective measures are needed.

Datatilsynet concluded under doubt that Telenor ASA had not ensured the DPO adequate resources under Article 38(2) GDPR, but since Telenor ASA does not have a DPO at the moment we do not impose a corrective measure for that.

13.2 **Compliance orders**

Based on the findings in section 13.1, we have concluded that it is necessary to react to these infringements. We order Telenor ASA:

- To carry out a documented internal assessment of whether Telenor ASA is obliged to appoint a DPO, which among other things, takes into account Telenor ASA's role in the various processing activities.

We refer to section 5.2.1, where we mention that Telenor ASA has not submitted a documented assessment of the matter of whether Telenor ASA is obliged to appoint a DPO in its roles as controller, joint controller and processor. Such an assessment shall be carried out as an organisational measure and documented as part of the internal control,[233] cf. Article 24 GDPR, unless it is obvious that it is not required.[234] Considering uncertainties surrounding Telenor ASA's role, as well as the fact that the company's record of processing activities includes far more processing activities with a greater scope than pure HR tasks in Telenor ASA and a high number of data subjects in several countries, we believe such an assessment is required.

- To revise the record of processing activities, cf. Article 30 GDPR, and implement organisational measures to ensure that it at all times reflects an updated description of

[233] Jarbekk et al. Eva Jarbekk et al.: *Personopplysningsloven og personvernforordningen med kommentarer* (2019), p. 256.
[234] WP 243 rev. 01 'Guidelines on Data Protection Officers', pp. 5–6

Telenor ASA's processing activities, the number of data subjects and Telenor ASA's roles.

We refer to sections 5.2.2 and 5.2.3, where we discuss Telenor ASA's record of processing activities. Keeping and maintaining such records, cf. Article 30 GDPR, also falls within the scope of the mandatory internal control and organisational measures that Telenor ASA must implement in accordance with Article 24 GDPR.[235] The record of processing activities is an important document that provides a genuine overview of the company's processing activities and roles.

- In the event that Telenor ASA is actually obliged to have a DPO, to implement organisational measures and appropriate policies with regard to the DPO's organisation. This includes a description of the reporting line to a clearly defined highest management level, a description of the tasks the DPO should be involved in, as well as the manner and timing of such involvement. Assessments and measures to ensure independence and to avoid conflicts of interest include clearly distinguishing between any other roles in the job description, providing a separate email address for the DPO and carrying out a documented assessment of the DPO's shareholding in the company.

We refer to section 12.

Our legal basis for imposing this compliance order is Article 58(2)(d) GDPR.

As mentioned, in order for processing activities to meet the requirements of the GDPR, it is a prerequisite that the controller meets all its obligations under Chapter IV GDPR. We therefore believe that the supervisory authority under Article 58(2) GDPR is not limited to processing activities as such, but includes all the requirements for GDPR compliance.[236] This is also supported by Article 57(1)a GDPR, that establish the Supervisory Authorities' task of monitoring and enforcing the application of the GDPR. CJEU has stated that use of corrective measures shall 'ensure a consistent and high level of protection of personal data through strong enforcement of the rules (…)' and the purpose of Article 58(2) GDPR is 'to ensure that the processing of personal data complies with that regulation and to make good situations where there has been a breach of that regulation so as to make them conform with EU law, as a result of intervention by the national supervisory authorities (…).' [237]

In any case, it is clear that Datatilsynet can impose administrative fine for a number of infringements which do not directly apply to specific processing activity as such. In some cases it is more appropriate and proportionate to impose milder administrative sanction as an

[235] Åste Marie Bergseng Skullerud, Cecilie Rønnevik, Jørgen Skorstad & Marius Engh Pellerud: *Personopplysningsloven og personvernforordningen (GDPR), kommentarutgave* (2019) p. 273 og 276, Eva Jarbekk et al.: *Personopplysningsloven og personvernforordningen med kommentarer* (2019) p. 257.
[236] On page 51 of the response of 31 May 2024, Telenor ASA stated that we cannot impose orders because the orders do not concern the performance of the processing activities.
[237] CJEU Case C-768/21 *Land Hessen*, para 38 og 45.

order than to impose an administrative fine. The same also applies to a reprimand, which Recital 148 explicitly states can be imposed instead of an administrative fine.

The questions concerning the appointment of a DPO and inaccuracies in the record of processing activities were not initially addressed specifically during the inspection, but were raised by Telenor ASA in its comments on the advance notification. We consider that it is not necessary and proportionate in relation to these infringements to impose an administrative fine.

The deadline for fulfilling the compliance orders is **3 months** from the date Telenor ASA received the decision, and we ask Telenor ASA to send us a documented confirmation that the compliance order has been fulfilled within that timeframe.

13.3 **Reprimand**

A reprimand is an administrative sanction intended to emphasise criticism of the cited infringements. Imposition of a reprimand may be emphasised in any subsequent assessments of whether to impose an administrative fine if there is a corresponding violation of the regulations, cf. Article 83(2)(i) GDPR.

The DPO plays an important role in assisting the controller/processor in ensuring compliance with the requirements of the GDPR and ensuring that the fundamental rights of the data subjects are safeguarded. The obligations in Article 38 GDPR are basic requirements that must be met in order to have a functional DPO. The requirements are the same regardless of whether the appointment of a DPO is mandatory or voluntary. We find that violation of these provisions leads to the inefficiency of the DPO, which again can affect the data subject's rights and to processing activities not complying with the law. In principle, this indicates that the supervisory authority can impose an administrative fine. In some cases, however, there are circumstances that indicate that a reprimand is an appropriate reaction.

As a consequence of the notification of the decision, Telenor ASA chose to terminate the DPO arrangement. In our view, this is very regrettable. We find this requires a more thorough assessment than what has been carried out, as it is not obvious that Telenor ASA is not required to have a DPO. If, following such an assessment, Telenor ASA maintains that their DPO role is voluntary, we will nonetheless encourage the company to reinstate the DPO. In particular, it should be taken into account that it emerged during the inspection and later that the DPO has in practice dedicated one hundred per cent of their time to the role, at the same time as there have been DPO tasks they have not been able to perform. Considering the company's own description of the need for data protection work, it is therefore a paradox that they choose to terminate the DPO role instead of ensuring that it is carried out both in accordance with the GDPR and allocated sufficient resources.

However, we agree with Telenor ASA that it can send an unfortunate signal beyond this case if an administrative fine is imposed for something that is a voluntary arrangement, and the threshold for this should therefore be high. The purpose of the DPO role is precisely to contribute to companies' compliance and maintaining a privacy culture, and Datatilsynet

would prefer more companies to have a DPO. We would nonetheless like to emphasise that the circumstances that were uncovered during the inspection and that we have assessed following further information from Telenor ASA indicate that Article 38(3) GDPR has been violated and that the violation provides a basis for an administrative fine. The case may therefore have been different if Telenor ASA clearly fell within the obligation to appoint a DPO set out in Article 37.

We consider it necessary to react to the violations, and taking into account the above, we impose a reprimand for violating Article 38(3) last sentence GDPR for

- not having a direct reporting line in place for the DPO in Telenor ASA to the highest management level for approximately one year of the timeframe of the inspection.

Our legal basis for imposing this reprimand order is Article 58(2)(d) GDPR.

13.4 Whether to impose an administrative fine

In what follows, we will consider whether to impose an administrative fine for infringements of violations of Article 24(1) and (2) GDPR, when it comes to inadequate organisational measures linked to Article 38 GDPR and general compliance with the GDPR.

13.4.1 General principles when assessing whether to impose administrative fines

An 'administrative sanction' is a negative reaction that may be imposed by an administrative agency in response to an actual breach of a statute, regulation or individual decision, and which is deemed to be a criminal sanction pursuant to the European Convention on Human Rights (ECHR).[238]

The Norwegian Supreme Court (Rt. 2012 p. 1556) has concluded that an administrative fine constitutes a penalty under Article 6 ECHR. As a result, we can only impose a fine where there is a clear preponderance of evidence (in Norwegian: 'klar sannsynlighetsovervekt') that the GDPR has been violated. In this case there is clear preponderance of evidence for all the infringements that an administrative fine will be imposed for.

In order to impose administrative sanctions, such as an administrative fine, the principle of legal certainty must be satisfied. The principle of legal certainty (in Norwegian: 'legalitetsprinsippet') is a general principle in both EEA Law[239] and Norwegian administrative law.[240]

The right to impose administrative fines is provided as a means of ensuring effective compliance with and enforcement of the Personal Data Act. It follows from Article 83(1) GDPR that administrative fines 'shall in each individual case be effective, proportionate and dissuasive'.

---

[238] Section 43 of the Norwegian Public Administration Act.
[239] EFTA Court, Case E-9/11 page 29 paragraph 99.
[240] The Norwegian Constitution Article 113.

In Recital 148, this is elaborated:

> 'In order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation.'

The conditions for imposing a fine are set out in Article 83 GDPR. The provision suggests that the imposition of an administrative fine shall be based on a discretionary overall assessment, but also sets guidelines for the exercise of discretion by highlighting elements that should be given special attention, cf. Article 83(2) (a) to (k) GDPR.

In its decision of 5 December 2023 in Case C-807/21 (*Deutsche Wohnen*), the CJEU specified that the conditions for imposing an administrative fine are exhaustively regulated by Article 83(1) to (6) GDPR. The Court concluded that Article 83 must be understood to mean that the imposition of an administrative fine is conditional on the controller having demonstrated culpability in the form of negligence or intent. The fee should be set so high that it also takes effect beyond the specific case, while the amount of the fee must proportionate to the infringement and the undertaking, cf. Article 83(1) GDPR.

In regard to the purpose of the provisions in the GDPR, CJEU has stated that it

> '… to ensure a consistent and high level of protection of natural persons with regard to the processing of personal data within the European Union and, to that end, to ensure consistent and homogeneous application of the rules for the protection of the fundamental rights and freedoms of those persons with regard to the processing of personal data throughout the European Union.'[241]
>
> 'Through their deterrent effect, administrative fines contribute to strengthening the protection of natural persons with regard to the processing of personal data and therefore constitute a key element in ensuring respect for the rights of those persons, in accordance with the purpose of that regulation of ensuring a high level of protection of such persons with regard to the processing of personal data.'[242]

13.4.2 **Statutory requirements**

Depending on the circumstances of each individual case, an administrative fine shall be imposed in accordance with Article 58(2)(i) GDPR, in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2), cf. Article 83(2) first sentence GDPR.

Article 24 GDPR is not mentioned in the list in Article 83(4) and (5) GDPR. Violations of this provision can therefore only be sanctioned with an administrative fine if so provided for in

[241] CJEU Case C-807/21 *Deutsche Wohnen v Staatsanwaltschaft Berlin*, para 72.
[242] CJEU Case C-807/21 *Deutsche Wohnen v Staatsanwaltschaft Berlin*, para 73.

national law. For Article 24 GDPR, such a legal basis is provided in Section 26 first paragraph of the Personal Data Act, cf. Article 84 GDPR.

13.4.3 **Elements to be given special emphasis when considering to impose a fine**
In assessing whether an administrative fine should be imposed, Datatilsynet must emphasise the elements in Article 83(2)(a) to (k) GDPR. Below is our assessment of the elements we consider relevant in assessing whether an administrative fine should be imposed for violations of Articles 24(1) and (2) GDPR.

a) *the nature, gravity and duration of the infringement*
As regards the criterion in Article 83(2)(a) GDPR, Telenor ASA's infringements as summarised above may be sanctioned in accordance with the lower tier of sanctions under the GDPR's two-tier sanctions system, cf. Article 83(4) GDPR.

When it comes to the nature of the infringements, the duty to implement appropriate organisational measures and appropriate policies pursuant to Article 24(1) and (2) GDPR, results of the fundamental accountability principle. The accountability principle underlies all of the company's obligations and is a prerequisite for real, systematic and effective compliance with the GDPR. Therefore, the infringement concerns a central and fundamental norm in the GDPR, which is aggravating.

When weighing the *gravity* of the infringements, we take into consideration the nature of the processing, which is business activity. We attribute more weight to the gravity of the infringement when there is a clear imbalance between the data subjects and the controller such as in this case, where most of the data subjects are employees.[243]

Regarding the scope of the processing as mentioned, it is unclear which processing activities Telenor ASA is controller for, which in turn affects the extent of the responsibility under Article 24 GDPR.

This lack of clarity also makes it difficult to establish the purpose of the processing. According to Telenor ASA, *the purpose* is mainly HR administration and processing of employees' personal data.

It is also difficult to estimate the number of data subjects who are affected. Telenor ASA has around 380 employees, but the exact number of data subjects affected is uncertain. Telenor ASA's Article 30 record, shows that the number of data subjects encompassed by the processing activities carried out by Telenor ASA in the timeframe of the inspection varied from a minimum of 1–25 data subjects to maximum 25,000–100,000.[244] In addition, all employees of the Group, approximately 15,000 data subjects, are affected by processing carried out by subsidiaries for which Telenor ASA, according to their record of processing activities, has joint controllership, cf. section 5.2.3.

[243] Guidelines 04/2022 on the calculation of administrative fines under the GDPR, p. **18.
[244] Telenor ASA's Article 30 record of 2 February 2022.

Furthermore, a very high number of customers are mentioned as data subjects in the record of processing activities in connection with joint controllership with Telenor's subsidiaries. In its response, Telenor ASA states that the entries in the records do not reflect reality. Datatilsynet notes the importance of records of processing activities providing a correct picture of processing activities in the organisation. This is because the company must maintain an overview itself and because such records are an important form of documentation for the supervisory authority's assessments.

Due to the ambiguities in the documentation Telenor ASA has submitted to Datatilsynet, we cannot determine how many data subjects are affected by the infringement.

Identifying specific damage is not necessary to be able to establish that a violation has occurred, but the *extent of damage* must be included as an element in the assessment. We find it mitigating that no specific damage to data subjects has been found, but keep in mind that it may be difficult for data subjects to know and find out whether their personal data have been processed in violation of the GDPR.

The assessment of the *duration* of the infringement is limited to the timeframe of the inspection, which is the period from 10 October 2020 to 28 January 2022. We will only take into account the duration of the violations within this period. We do not take the situation before or after this period into consideration as aggravating or mitigating factors in this context.

The violation of Article 24(1) and (2) GDPR regarding organisational measures and appropriate policies lasted the entire timeframe of the inspection. We refer to section 12.2.

We find the duration of non-compliance of around 15 months in this case to be an aggravating factor.

Despite that it is not possible to demonstrate tangible damage to the data subject's privacy, as well as ambiguities regarding the processing's scope and purpose and the number of data subjects, we find that the nature and duration warrant the imposition of an administrative fine.

b) the intentional or negligent character of the infringement
The imposition of an administrative fine is conditional on the controller having demonstrated culpability in the form of negligence or intent, cf. Article 83(2)(b) GDPR in conjunction with Article 83(3) GDPR, cf. the CJEU's decisions dated 5 December 2023 in case 807/21 *Deutsche Wohnen* and C-683/21. In the Deutsche Wohnen decision CJEU states:

> 'Accordingly, it follows from the wording of Article 83(2) of the GDPR that only infringements of the provisions of that regulation committed wrongfully by the controller, that is to say those committed intentionally or negligently, can result in a fine being imposed on the controller pursuant to that article.'[245]

[245] CJEU Case C-807/21 *Deutsche Wohnen v Staatsanwaltschaft Berlin*, para 68.

See also the Norwegian Public Administration Act section 46(1).

Negligence is defined as follows in Section 23 of the Penal Code:

> 'Any person who acts in contravention of the requirement of due care in an area of life, and who may be held to blame in view of his or her personal circumstances, is negligent. The negligence is gross if the act is highly reproachable and there are grounds for significant blame.'

Pursuant to the due care requirement, businesses and the responsible individuals acting on their behalf need to examine the legal requirements that apply to their field and implement these. Otherwise, the company can be deemed to have acted negligently with respect to this omission.

Telenor Group is a leading telecom company across the Nordics and Asia with 209 million subscribers and annuals sales of around NOK 81 billion (2023),[246] where Telenor ASA is the parent company located in Norway. In our view, Telenor ASA has the means and competence to familiarise itself with the legal requirements in the field of data protection, and should act accordingly.

In our view, Telenor ASA has not sufficiently familiarised itself with the requirements of Article 24 GDPR, as evidenced by the inadequate assessments, measures and policies. The information we got during the inspection shows that the company did not prioritise and allocate enough resources to address the problems identified by the external DPO, including with regard to internal control, despite clearly being encouraged to do so. In other words, the company has not done what could be expected, and it has not operated in accordance with the due care requirement. Therefore, the infringement was at least committed negligently. Consequently, we find a culpable infringement to have been established, which is a condition for imposing an administrative fine.[247]

We find that the culpability requirement has been met and that this indicates that an administrative fine should be imposed.

c) any action taken by the controller or processor to mitigate the damage suffered by data subjects

There is no evidence that the data subjects have suffered any material damage. This criterion is therefore not applicable in the present case.

d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32

[246] https://www.telenor.com/about/, last reviewed 11 April 2024.
[247] CJEU Case C-807/21 *Deutsche Wohnen v Staatsanwaltschaft Berlin*, para 75.

We agree with Telenor ASA that this criterion does not apply in this supervisory case, as technical and organisational measures pursuant to Articles 25 and 32 GDPR have not been an issue.

e) any relevant previous infringements by the controller or processor

This criterion is not applicable in the present case, as Telenor ASA has not been sanctioned for similar or otherwise 'relevant' infringements in the past.

f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement

Telenor ASA has been cooperative through the whole inspection, by providing information and answering our questions. We consider that this factor is neither an aggravating nor a mitigating factor.[248]

g) the categories of personal data affected by the infringement

Categories of personal data relating to Telenor ASA's own employees include contact information, information about career and competence, communication, location, behaviour, financial accounts and balance, financial transactions and family relations.[249] Some of these categories of personal data may be regarded as sensitive for the data subject (such as information about finances), even though they do not fall under Article 9(1) GDPR.

Only some of the categories fall within the definition of special categories of personal data pursuant to Article 9(1) GDPR, including health data relating to employees and the police records of job applicants.[250]

Categories of personal data relating to customers include behaviour, preferences, interests, demography, identity, location and physical characteristics (not health-related).[251] Telenor ASA also processes some categories of personal data relating to other persons, including consultants and contractors.[252]

It is difficult to conclude exactly which categories of personal data are affected by the infringement, because of ambiguity in the submitted documentation from Telenor ASA.

We find this criterion in sum, to be neither an aggravating nor a mitigating factor.

---

[248] According to WP253 Guidelines on the application and setting of administrative fines in accordance with Regulation (EU) 2016/679, p. 15, letter (f) may be a mitigating factor in some cases, but it would not be appropriate to take into account cooperation that is already required by law.
[249] Final inspection report of 30 September 2022, p. 5.
[250] Final inspection report of 30 September 2022, p. 5.
[251] Final inspection report of 30 September 2022, p. 5.
[252] Telenor ASA's Article 30 record of 2 February 2022.

h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement

The infringement became known to Datatilsynet through our own initiation of the inspection. In this case, we consider this to be neither an aggravating nor a mitigating factor.

i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures

This is neither a mitigating nor an aggravating factor, as we have not ordered any previously corrective measures against Telenor ASA with regard to the same subject matter.

j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42

This criterion is not applicable in the present case.

k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement

Datatilsynet has no information to indicate that Telenor ASA has benefitted financially from the infringements.

As explained previously, it is difficult to conclude various elements above because the scope of Telenor AS's controllership is ambiguous. This is a consequence of Telenor ASA not having implemented adequate organisational measures to maintain and update a record of processing activities, cf. section 5 and 13.2. Datatilsynet considers this to be an aggravating factor.

As described in the previous sections, Telenor ASA has taken some measures throughout 2021 and tried improving the reporting line for the DPO and added the option of escalating matters to the CEO and the board. These are considered mitigating factors.

13.4.4 **Conclusion on whether to impose an administrative fine**

Telenor ASA is the parent company of a large group in a strictly regulated telecom industry and should be equipped to have good internal control. Considering the factors set out in Article 83(2) GDPR, the imposition of an administrative fine is warranted due to the circumstances of this case.

In Datatilsynet's view, the imposition of an administrative fine will produce a genuine deterrent effect and dissuade Telenor ASA – as well as Telenor Group companies and other companies in general – from committing similar infringements in the future, and ensure that

they ensure good internal control, including the implementation of necessary measures and assessments as well as documentation thereof. Enforcement efforts should generate sufficient pressure to make non-compliance economically unattractive in practice.[253]

13.5 **Deciding the amount of the administrative fine**

Having had due regard to the factors under Articles 83(1) and (2) GDPR outlined above, we find an administrative fine of ***4,000,000 NOK*** to be appropriate in this case. The reasons for this are outlined below.

In that connection, it should be noted that the setting of a fine is not a precise mathematical exercise,[254] and the supervisory authorities have a certain margin of discretion in this respect.[255] They should nonetheless specify the factors that influenced the exercise of their discretion when setting a fine.[256]

Article 83(1) GDPR establishes the following when deciding the amount of administrative fines:

> 'Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.'

Article 83(2) GDPR further provides that, when deciding on the amount of the administrative fine in each individual case, due regard shall be given to the factors listed in Articles 83(2)(a)–(k) GDPR.

Recital 148 GDPR emphasises that administrative fines should be imposed 'in order to strengthen the enforcement of the rules of this Regulation'.

Recital 150 GDPR states:

> 'Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes.'

Pursuant to CJEU case law, the term 'undertaking' must be understood as an economic unit, even if that economic unit consists of several legal persons.[257] Different companies belonging

---

[253] See the Opinion of Advocate General Geelhoed in Case C-304/02, *Commission v France*, delivered on 29 April 2004, para 39.
[254] See, *inter alia*, CJEU Case T-425/18, *Altice Europe NV v Commission*, para 362; CJEU Case T-11/06, *Romana Tabacchi v Commission*, para 266.
[255] See, *inter alia*, CJEU Case T-192/06, *Caffaro Srl v Commission*, para 38.
[256] EDPB Decision 01/2022 on the dispute arisen on the draft decision of the French Supervisory Authority regarding Accor SA under Article 65(1)(a) GDPR para 75.
[257] CJEU Case C-516/15 P *Akzo Nobel and Others v Commission*, para 48, with further references. CJEU Case C-807/21 *Deutsche Wohnen v Staatsanwaltschaft Berlin*, para 56.

to the same group forming an economic unit is therefore considered an 'undertaking' within the meaning of Articles 101 and 102 TFEU (Treaty on the Functioning of the European Union).

Telenor ASA is the parent company of Telenor Group. Telenor Group must be considered an economic unit, and therefore also the SEU (single economic unit), i.e. the undertaking that is relevant for the calculation of the administrative fine.[258] The EDPB has issued a binding decision with the instruction to the supervisory authority to take into consideration the total turnover of all the entities composing the single undertaking, i.e. the consolidated turnover of the group of companies headed by the parent company.[259] The CJEU has ruled that the maximum amount of the administrative fine is calculated on the basis of a percentage of the total worldwide annual turnover in the preceding business year of the undertaking concerned.[260] The infringements found in this case qualify for administrative fines under Article 83(4) GDPR, pursuant to litra (a) of the provision. The maximum amount under Article 83(4) GDPR is 10,000,000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, *whichever is higher*.

In terms of the requirements under Article 83(1) GDPR to ensure that the imposition of the fine is effective, proportionate and dissuasive, the financial position of Telenor Group must be taken into account. The financial position of Telenor Group is also relevant to determine the maximum fine applicable in the present case.

In the calculation of the administrative fine, Datatilsynet takes into account the revenue of Telenor Group.[261] According to the financial statement of Telenor Group's annual report 2023, the group's total revenue in 2023 was NOK 80,452,000,000,[262] or approximately EUR 7,157,332,860.[263] In the present case, the legal maximum amount pursuant to Article 83(4) GDPR is 2% of the total annual turnover, which in 2023 amounted to NOK 1,609,040,000, or approximately EUR 143,146,000.[264]

We refer to our assessments above in this section on the factors set out in Articles 83(2)(a)–(k) GDPR. It is very important that a controller maintains good internal control, carries out necessary assessments that are documented and establishes the necessary organisational measures, which we have found to be lacking during the timeframe of the inspection.

---

[258] EDPB Guidelines 04/2022 on the calculation of administrative fines under the GDPR, p. 38.
[259] EDPB Binding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook service (Art. 65 GDPR), adopted on 13 April 2023, para 365.
[260] CJEU Case C-807/21 *Deutsche Wohnen v Staatsanwaltschaft Berlin*, para 57.
[261] EDPB Guidelines 04/2022 on the calculation of administrative fines under the GDPR, p. 38; EDPB, Binding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook service (Art. 65 GDPR), adopted on 13 April 2023, para 365.
[262] In the previous notification (in English), the annual report for 2022 was used as a basis because the annual report for 2023 had not been published. The notification has been updated with information from the 2023 annual report.
[263] Based on the EUR to NOK daily exchange rate on 29 December 2023 of 11.2405, quoted by Norges Bank: Exchange rates (norges-bank.no), last visited 11 April 2024.
[264] Based on the EUR to NOK daily exchange rate on 29 December 2023 of 11.2405, quoted by Norges Bank: Exchange rates (norges-bank.no), last visited 11 April 2024.

Emphasis is also placed on Telenor ASA's negligence (Article 83(2)(b)), especially in view of the company's size and influence and what is expected of such a company. That said, we have not found direct damage to data subjects. This is a factor we give considerable weight.

We have moreover emphasised that the processing time has been long and the case has been inactive for some time, which implies downward adjustment to the amount. This is also in accordance with the practice of the Privacy Appeals Board; see the decisions in cases PVN-2022-3, PVN-2021-20, PVN-2021-16, PVN-2021-13 and PVN-2021-3.

In sum we are of the opinion that the administrative fine should be set at low level.

We believe that an administrative fine of NOK 4,000,000, or approximately 0.005% of Telenor Group's annual turnover, is proportionate and dissuasive in this case, in light of the specific circumstances. The amount does not exceed what is necessary to achieve compliance with the GDPR in this case.

14 Collection of the administrative fine

The administrative fine is due for payment four weeks after the decision is final, cf. the Personal Data Act (2018) Section 27. The decision constitutes grounds for an attachment order. Collection of the claim will be carried out by the Norwegian National Collection Agency.

15 European cooperation

This decision has been adopted in cooperation with the other concerned supervisory authorities, pursuant to Article 60 GDPR.

16 Access to documents

Pursuant to the Public Administration Act Sections 18 and 19, Telenor ASA – as a party to this case – has the right to acquaint itself with the documents in this case. Documents in the case were submitted on 22 December 2021 and 22 March 2024.

Pursuant to Section 3 of the Freedom of Information Act,[265] all case documents we hold are, as a rule, subject to public access. If you think that any documents in this case should be partly or entirely exempted from public access based on legal derogations, please notify us and provide an explanation for your claim.

17 Right to appeal

When a decision has been adopted pursuant to Article 56(2) GDPR and Chapter VII GDPR, it may be challenged before Oslo District Court ('Oslo tingrett') in accordance with Article

[265] Act No 16 of 19 May 2006 relating to the right of access to documents held by public authorities and public undertakings (Freedom of Information Act)

78(1) GDPR, Sections 22 and 25 of the Personal Data Act and Section 4-4(4) of the Dispute Act.[266]

Yours sincerely,

Mona Naomi Lintvedt
Acting Director General

Anna Kristin Ulfarsdottir
Legal Specialist Adviser

This document has been electronically approved and therefore carries no handwritten signatures

[266] Act No 90 of 17 June 2005 relating to mediation and procedure in civil disputes (Dispute Act).